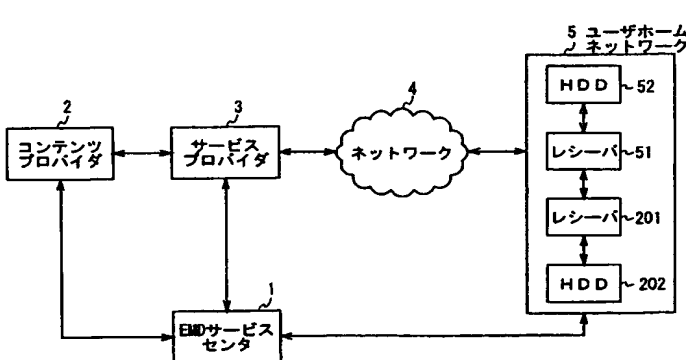


<b>(51) 国際特許分類7</b> <b>G06F 17/60</b>	<b>A1</b>	<b>(11) 国際公開番号</b> <b>WO00/62218</b>  <b>(43) 国際公開日</b> 2000年10月19日(19.10.00)
<b>(21) 国際出願番号</b> PCT/JP00/02291  <b>(22) 国際出願日</b> 2000年4月7日(07.04.00)  <b>(30) 優先権データ</b> 特願平11/103339 1999年4月9日(09.04.99) JP  <b>(71) 出願人</b> (米国を除くすべての指定国について) ソニー株式会社(SONY CORPORATION)[JP/JP] 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo, (JP) <b>(72) 発明者 ; および</b> <b>(75) 発明者 / 出願人</b> (米国についてののみ) 石橋義人(ISHIBASHI, Yoshihito)[JP/JP] 浅野智之(ASANO, Tomoyuki)[JP/JP] 北村 出(KITAMURA, Iduru)[JP/JP] 北原 淳(KITAHARA, Jun)[JP/JP] 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo, (JP) <b>(74) 代理人</b> 弁理士 田辺恵基(TANABE, Shigemoto) 〒150-0001 東京都渋谷区神宮前1丁目11番11-508号 グリーンフアンタジアビル5階 Tokyo, (JP)		<b>(81) 指定国</b> CN, KR, SG, US, 欧州特許 (DE, FR, GB)  添付公開書類 国際調査報告書
<b>(54) Title: INFORMATION PROCESSING DEVICE AND METHOD, AND PROVIDING MEDIUM</b>  <b>(54) 発明の名称</b> 情報処理装置および方法、並びに提供媒体  <div style="text-align: center;">  </div> <div style="text-align: center;"> <p>1...END SERVICE CENTER          2...CONTENTS PROVIDER          3...SERVICE PROVIDER          4...NETWORK          5...USER HOME NETWORK          51...RECEIVER          201...RECEIVER</p> </div>		
<b>(57) Abstract</b> A main information processing device can settle a charge in place of an information processing device connected therewith. In place of a receiver (201) incapable of settling a charge, a receiver (51) settles the charge which is calculated by the receiver (201).		

(57)要約

主の情報処理装置が、それに接続される情報処理装置に代わって、課金を決済する処理を行うことができるようにする。課金を決済する処理を行うことができないレシーバ201に代わって、レシーバ201において計上された課金を決済する処理を、レシーバ51が行う。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE	アラブ首長国連邦	DM	ドミニカ	KZ	カザフスタン	RU	ロシア
AG	アンティグア・バーブーダ	DZ	アルジェリア	LC	セントルシア	SD	スーダン
AL	アルバニア	EE	エストニア	LI	リヒテンシュタイン	SE	スウェーデン
AM	アルメニア	ES	スペイン	LK	スリ・ランカ	SG	シンガポール
AT	オーストリア	FI	フィンランド	LR	リベリア	SI	スロヴェニア
AU	オーストラリア	FR	フランス	LS	レソト	SK	スロヴァキア
AZ	アゼルバイジャン	GA	ガボン	LT	リトアニア	SL	シエラ・レオネ
BA	ボスニア・ヘルツェゴビナ	GB	英国	LU	ルクセンブルグ	SN	セネガル
BB	バルバドス	GD	グレナダ	LV	ラトヴィア	SZ	スワジランド
BE	ベルギー	GE	グルジア	MA	モロッコ	TD	チャード
BF	ブルキナ・ファソ	GH	ガーナ	MC	モナコ	TG	トーゴ
BG	ブルガリア	GM	ガンビア	MD	モルドヴァ	TJ	タジキスタン
BJ	ベナン	GN	ギニア	MG	マダガスカル	TM	トルクメニスタン
BR	ブラジル	GR	ギリシャ	MK	マケドニア旧ユーゴスラヴィア	TR	トルコ
BY	ベラルーシ	GW	ギニア・ビサウ		共和国	TT	トリニダード・トバゴ
CA	カナダ	HR	クロアチア	ML	マリ	TZ	タンザニア
CC	中央アフリカ	HU	ハンガリー	MN	モンゴル	UA	ウクライナ
CG	コンゴ	ID	インドネシア	MR	モーリタニア	UG	ウガンダ
CH	スイス	IE	アイルランド	MW	マラウイ	US	米国
CI	コートジボアール	IL	イスラエル	MX	メキシコ	UZ	ウズベキスタン
CM	カメルーン	IN	インド	MZ	モザンビーク	VN	ヴェトナム
CN	中国	IS	アイスランド	NE	ニジェール	YU	ユーゴスラヴィア
CU	キューバ	IT	イタリア	NL	オランダ	ZA	南アフリカ共和国
CY	キプロス	JP	日本	NO	ノールウェー	ZW	ジンバブエ
CZ	チェコ	KE	ケニア	NZ	ニュージーランド		
DE	ドイツ	KG	キルギスタン	PL	ポーランド		
DK	デンマーク	KP	北朝鮮	PT	ポルトガル		
		KR	韓国	RO	ルーマニア		

## 明 細 書

### 情報処理装置および方法、並びに提供媒体

#### 技術分野

本発明は、情報処理装置および方法、並びに提供媒体に関し、特に、暗号化された情報を利用する情報処理装置および方法、並びに提供媒体に関する。

#### 背景技術

音楽などの情報（以下、コンテンツと称する）を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザが、情報処理装置でコンテンツを復号して、利用するシステムがある。

複数の情報処理装置を有している場合、ユーザは、それぞれの情報処理装置毎に、コンテンツを購入し、その利用料金を精算しなければならない、手間がかかる課題があった。

#### 発明の開示

本発明はこのような状況に鑑みてなされたものであり、ユーザが複数の情報処理装置を有している場合、主とする情報処理装置を利用して、他の情報処理装置で利用されるコンテンツを購入したり、料金の精算をすることができるようにするものである。

かかる課題を解決するため本発明においては、情報処理装置において、他の情報処理装置の所定の代理決済情報を記憶する記憶手段と、記憶手段に記憶されている代理決済情報に対応して、所定の課金情報の提供を他の情報処理装置に要求する要求手段と、要求手段による要求に応じて、他の情報処理装置から送信されてくる課金情報を受信する第1の受信手段と、第1の受信手段により受信された課金情報を、管理装置に送信する送信手段と、管理装置から送信されてくる、送

信手段により送信された課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件を受信する第2の受信手段と、第2の受信手段により受信された登録条件に基づいて、動作を制御する制御手段とを具備する。

また本発明においては、情報処理方法において、他の情報処理装置の所定の代理決済情報を記憶する記憶ステップと、記憶ステップで記憶された代理決済情報に対応して、所定の課金情報の提供を他の情報処理装置に要求する要求ステップと、要求ステップでの要求に応じて、他の情報処理装置から送信されてくる課金情報を受信する第1の受信ステップと、第1の受信ステップで受信された課金情報を、管理装置に送信する送信ステップと、管理装置から送信されてくる、送信ステップで送信された課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件を受信する第2の受信ステップと、第2の受信ステップで受信された登録条件に基づいて、動作を制御する制御ステップとを具備する。

さらに本発明においては、提供媒体において、他の情報処理装置の所定の代理決済情報を記憶する記憶ステップと、記憶ステップで記憶された代理決済情報に対応して、所定の課金情報の提供を他の情報処理装置に要求する要求ステップと、要求ステップでの要求に応じて、他の情報処理装置から送信されてくる課金情報を受信する第1の受信ステップと、第1の受信ステップで受信された課金情報を、管理装置に送信する送信ステップと、管理装置から送信されてくる、送信ステップで送信された課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件を受信する第2の受信ステップと、第2の受信ステップで受信された登録条件に基づいて、動作を制御する制御ステップとを具備する処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

さらに本発明においては、情報処理装置、情報処理方法、および提供媒体においては、他の情報処理装置の所定の代理決済情報が記憶され、記憶された代理決済情報に対応して、所定の課金情報の提供が他の情報処理装置に要求され、要求に応じて、他の情報処理装置から送信されてくる課金情報が受信され、受信され

た課金情報が、管理装置に送信され、管理装置から送信されてくる、送信された課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件が受信され、受信された登録条件に基づいて、動作が制御される。

さらに本発明においては、情報処理装置において、他の情報処理装置の所定の代理購入情報を記憶する第１の記憶手段と、第１の記憶手段に記憶されている代理購入情報に対応して、所定の課金情報を作成する第１の作成手段と、第１の記憶手段に記憶されている代理購入情報に対応して、所定の使用許諾条件情報を作成する第２の作成手段と、第１の作成手段により作成された課金情報を記憶する第２の記憶手段と、第２の作成手段により作成された使用許諾条件情報と、管理装置から供給された、暗号化された情報を復号するために必要な鍵を、他の情報処理装置に送信する送信手段とを具備する。

さらに本発明においては、情報処理方法において、他の情報処理装置の所定の代理購入情報を記憶する第１の記憶ステップと、第１の記憶ステップで記憶された代理購入情報に対応して、所定の課金情報を作成する第１の作成ステップと、第１の記憶ステップで記憶された代理購入情報に対応して、所定の使用許諾条件情報を作成する第２の作成ステップと、第１の作成ステップで作成された課金情報を記憶する第２の記憶ステップと、第２の作成ステップで作成された使用許諾条件情報と、管理装置から供給された、暗号化された情報を復号するために必要な鍵を、他の情報処理装置に送信する送信ステップとを含むことを特徴とする。

さらに本発明においては、提供媒体において、他の情報処理装置の所定の代理購入情報を記憶する第１の記憶ステップと、第１の記憶ステップで記憶された代理購入情報に対応して、所定の課金情報を作成する第１の作成ステップと、第１の記憶ステップで記憶された代理購入情報に対応して、所定の使用許諾条件情報を作成する第２の作成ステップと、第１の作成ステップで作成された課金情報を記憶する第２の記憶ステップと、第２の作成ステップで作成された使用許諾条件情報と、管理装置から供給された、暗号化された情報を復号するために必要な鍵を、他の情報処理装置に送信する送信ステップとを具備する処理を実行させるコ

ンピュータが読み取り可能なプログラムを提供することを特徴とする。

さらに本発明においては、情報処理装置、情報処理方法、および提供媒体においては、他の情報処理装置の所定の代理購入情報が記憶され、記憶されている代理購入情報に対応して、所定の課金情報が作成され、記憶されている代理購入情報に対応して、所定の使用許諾条件情報が作成され、作成された課金情報が記憶され、作成された使用許諾条件情報と、管理装置から供給された、暗号化された情報を復号するために必要な鍵を、他の情報処理装置に送信する送信手段とを具備する。

#### 図面の簡単な説明

図1は、EMDシステムを説明する系統図である。

図2は、EMDシステムにおける、主な情報の流れを説明する系統図である。

図3は、EMDサービスセンタ1の機能的構成を示すブロック系統図である。

図4は、EMDサービスセンタ1の配送用鍵Kdの送信を説明する略線図である。

図5は、EMDサービスセンタ1の配送用鍵Kdの送信を説明する他の略線図である。

図6は、EMDサービスセンタ1の配送用鍵Kdの送信を説明する他の略線図である。

図7は、EMDサービスセンタ1の配送用鍵Kdの送信を説明する他の略線図である。

図8は、コンテンツプロバイダ2の機能的構成例を示すブロック系統図である。

図9は、UCPを説明する図表である。

図10は、コンテンツの管理移動を説明する略線図である。

図11は、第1世代複製を説明する略線図である。

図12は、サービスコードおよびコンディションコードのコード値の例を示す

図表である。

図 1 3 は、U C P の利用条件として設定されたコード値の例を示す図表である。

図 1 4 は、コンテンツプロバイダセキュアコンテナの例を示す略線図である。

図 1 5 は、コンテンツプロバイダ 2 の証明書の例を示す略線図である。

図 1 6 は、サービスプロバイダ 3 の機能の構成を示すブロック図である。

図 1 7 は、P T の例を示す図表である。

図 1 8 は、P T の価格条件として設定されたコード値の例を示す図表である。

図 1 9 は、他の P T の例を示す図表である。

図 2 0 は、他の P T の価格条件として設定されたコード値の例を示す図表である。

図 2 1 は、サービスプロバイダセキュアコンテナの例を示す略線図である。

図 2 2 は、サービスプロバイダ 3 の証明書の例を示す略線図である。

図 2 3 は、ユーザホームネットワーク 5 のレシーバ 5 1 の機能的構成例を示すブロック図である。

図 2 4 は、レシーバ 5 1 の S A M 6 2 の証明書の例を示す略線図である。

図 2 5 は、U C S の例を示す図表である。

図 2 6 は、レシーバ 5 1 の外部記憶部 6 3 の利用情報記憶部 6 3 A の内部を説明する略線図である。

図 2 7 は、課金情報の例を示す図表である。

図 2 8 は、レシーバ 5 1 の記憶モジュール 7 3 に記憶されている情報を示す図表である。

図 2 9 は、基準情報 5 1 を説明する図表である。

図 3 0 は、レシーバ 5 1 の登録リストの例を示す図表である。

図 3 1 は、ユーザホームネットワーク 5 のレシーバ 2 0 1 の機能的構成例を示すブロック図である。

図 3 2 は、レシーバ 2 0 1 の登録リストの例を示す図表である。

図 3 3 は、コンテンツの利用処理を説明するフローチャートである。

図 3 4 は、EMD サービスセンタ 1 がコンテンツプロバイダ 2 へ配送用鍵 K d を送信する処理を説明するフローチャートである。

図 3 5 は、コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の動作を説明するフローチャートである。

図 3 6 は、コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の他の動作を説明するフローチャートである。

図 3 7 は、コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の他の動作を説明するフローチャートである。

図 3 8 は、コンテンツプロバイダ 2 がサービスプロバイダ 3 にコンテンツプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

図 3 9 は、サービスプロバイダ 3 がレシーバ 5 1 にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

図 4 0 は、レシーバ 5 1 がサービスプロバイダセキュアコンテナを受信する処理を説明するフローチャートである。

図 4 1 は、レシーバ 5 1 がコンテンツを再生する処理を説明するフローチャートである。

図 4 2 は、課金を決済する処理を説明するフローチャートである。

図 4 3 は、代理決済処理の手順を説明するフローチャートである。

図 4 4 は、代理決済処理の手順を説明するフローチャートである。

図 4 5 は、代理決済処理の手順を説明するフローチャートである。

図 4 6 は、ユーザホームネットワーク 5 の他の構成例を示す系統図である。

図 4 7 は、ユーザホームネットワーク 5 のレシーバ 5 1 の登録リストの例を示す図表である。

図 4 8 は、ユーザホームネットワーク 5 のレシーバ 2 5 1 の登録リストの例を示す図表である。

図 4 9 は、代理決済処理の他の手順を説明するフローチャートである。

図50は、代理決済処理の他の手順を説明するフローチャートである。

図51は、代理決済処理の他の手順を説明するフローチャートである。

図52は、ユーザホームネットワーク5の他の構成例を示す系統図である。

図53は、レシーバ301の構成例を示す系統図である。

図54は、レシーバ301の利用情報記憶部312Aの形態を示す略線図である。

図55は、レシーバ301の登録リストの例を示す図表である。

図56は、レシーバ401の構成例を示す系統図である。

図57は、レシーバ401の登録リストの例を示す図表である。

図58は、レシーバ51の登録リストの例を示す図表である。

図59は、代理購入処理の手順を説明するフローチャートである。

図60は、代理購入処理の他の手順を説明するフローチャートである。

図61は、代理購入処理の他の手順を説明するフローチャートである。

図62は、代理購入処理の他の手順を説明するフローチャートである。

図63は、代理購入処理の他の手順を説明するフローチャートである。

#### 発明を実施するための最良の形態

以下に本発明の実施の形態を説明する。

##### (1) 情報配信システム

図1は、本発明を適用したEMD (Electronic Music Distribution: 電子音楽配信) システムを説明する図である。EMDシステムは、各装置を管理するEMDサービスセンタ1、コンテンツを提供するコンテンツプロバイダ2、コンテンツに対応する所定のサービスを提供するサービスプロバイダ3、およびコンテンツが利用される機器 (この例の場合、HDD52に接続されているレシーバ51およびHDD202に接続されているレシーバ201) からなるユーザネットワーク5から構成されている。

EMDシステムにおけるコンテンツ (Content) とは、情報そのものが

価値を有するデジタルデータで、この例の場合、1つのコンテンツは、1曲分の音楽データに相当する。尚、コンテンツは、音楽データだけでなく、映像データ、ゲームプログラム、コンピュータプログラム、著作データなどの場合も有りうる。

EMDサービスセンタ1は、EMDシステムにおける主な情報の流れを示す図2に示すように、ユーザホームネットワーク5およびコンテンツプロバイダ2に、コンテンツを利用するために必要な配送用鍵Kdを送信する。EMDサービスセンタ1はまた、ユーザホームネットワーク5の機器から、課金情報等を受信して、料金を精算する処理などを実行する。

コンテンツプロバイダ2は、提供するコンテンツ（コンテンツ鍵Kcoで暗号化されている）、そのコンテンツを復号するために必要なコンテンツ鍵Kco（配送用鍵Kdで暗号化されている）、およびコンテンツの利用内容などを示す取扱方針（以下、UCP（Usage Control Policy）と記述する）を保持し、それらを、コンテンツプロバイダセキュアコンテナ（後述）と称する形態で、サービスプロバイダ3に供給する。

サービスプロバイダ3は、コンテンツプロバイダ2から供給されるUCPの利用内容に対応して、1つまたは複数の価格情報（以下、PT（Price Tag）と記述する）を作成し、保持する。サービスプロバイダ2は、作成したPTを、コンテンツプロバイダ2から供給されたコンテンツ（コンテンツ鍵Kcoで暗号化されている）、コンテンツ鍵Kco（配送用鍵Kdで暗号化されている）、およびUCPとともに、サービスプロバイダセキュアコンテナと称する形態で、専用のケーブルネットワーク、インターネット、または衛星通信などから構成されるネットワーク4を介して、ユーザホームネットワーク5に送信する。

ユーザホームネットワーク5は、供給されたUCPおよびPTに基づいて、使用許諾条件情報（以下、UCS（Usage Control Status）と称する）を作成し、作成したUCSに基づいてコンテンツを利用する処理を実行する。ユーザホームネットワーク5はまた、UCSを作成するタイミングで課

金情報を作成し、例えば、配送用鍵K dの供給を受けるタイミングで、EMDサービスセンタ1に送信する。

## (2) EMDサービスセンタ

図3は、EMDサービスセンタ1の機能的構成を示すブロック図である。サービスプロバイダ管理部11は、サービスプロバイダ3に利益分配の情報を供給する。コンテンツプロバイダ管理部12は、コンテンツプロバイダ2に配送用鍵K dを送信したり、利益分配の情報を供給する。

著作権管理部13は、ユーザホームネットワーク5のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、JASRAC (Japanese Society For Rights of Authors, Composer S And Publishers : 日本音楽著作権協会)に送信する。

鍵サーバ14は、配送用鍵K dを記憶しており、それを、コンテンツプロバイダ管理部12を介してコンテンツプロバイダ2に供給したり、ユーザ管理部18等を介してユーザホームネットワーク5に供給する。

ユーザホームネットワーク5の機器およびコンテンツプロバイダ2に供給される、EMDサービスセンタ1からの配送用鍵K dについて、図4乃至図7を参照して説明する。

図4は、コンテンツプロバイダ2がコンテンツの提供を開始し、ユーザホームネットワーク5を構成するレシーバ51がコンテンツの利用を開始する、1998年1月における、EMDサービスセンタ1が有する配送用鍵K d、コンテンツプロバイダ2が有する配送用鍵K d、およびレシーバ51が有する配送用鍵K dを示す図である。

図4の例において、配送用鍵K dは、暦の月の初日から月の末日まで、使用可能であり、たとえば、所定のビット数の乱数である“aaaaaaaa”の値を有するバージョン1である配送用鍵K dは、1998年1月1日から1998年1月31日まで使用可能（すなわち、1998年1月1日から1998年1月3

1日の期間にサービスプロバイダ3を介してユーザホームネットワーク5に配布されるコンテンツを暗号化するコンテンツ鍵Kcは、バージョン1である配送用鍵Kdで暗号化されている)であり、所定のビット数の乱数である“bbbbbbbb”の値を有するバージョン2である配送用鍵Kdは、1998年2月1日から1998年2月28日まで使用可能(すなわち、その期間にサービスプロバイダ3を介してユーザホームネットワーク5に配布されるコンテンツを暗号化するコンテンツ鍵Kcは、バージョン2である配送用鍵Kdで暗号化されている)である。同様に、バージョン3である配送用鍵Kdは、1998年3月中に使用可能であり、バージョン4である配送用鍵Kdは、1998年4月中に使用可能であり、バージョン5である配送用鍵Kdは、1998年5月中に使用可能であり、バージョン6である配送用鍵Kdは、1998年6月中に使用可能である。

コンテンツプロバイダ2がコンテンツの提供を開始するに先立ち、EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年1月から1998年6月まで利用可能な、バージョン1乃至バージョン6の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、記憶する。6ヶ月分の配送用鍵Kdを記憶するのは、コンテンツプロバイダ2が、コンテンツを提供する前のコンテンツおよびコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

また、レシーバ51がコンテンツの利用を開始するに先立ち、EMDサービスセンタ1は、レシーバ51に、1998年1月から1998年3月まで、利用可能なバージョン1乃至バージョン3である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、記憶する。3ヶ月分の配送用鍵Kdを記憶するのは、レシーバ51が、EMDサービスセンタ1に接続できないなどのトラブルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用できない等の事態を避けるためであり、また、EMDサービスセンタ1への接続の頻度を低くし、ユーザホームネットワーク5の負荷を低減するためである。

る。

1998年1月1日から1998年1月31日の期間には、バージョン1である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

1998年2月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2、およびレシーバ51への送信を図5で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年2月から1998年7月まで利用可能な、バージョン2乃至バージョン7の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年2月から1998年4月まで、利用可能なバージョン2乃至バージョン4である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵Kdをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送用鍵Kdを利用できるようにするためである。

1998年2月1日から1998年2月28日の期間には、バージョン2である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

1998年3月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2、およびレシーバ51への送信を図6で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年3月から1998年8月まで利用可能な、バージョン3乃至バージョン8の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年3月から1998年5月まで、利

用可能なバージョン3乃至バージョン5である3つの配送用鍵K dを送信し、レシーバ5 1は、3つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵K dおよびバージョン2である配送用鍵K dをそのまま記憶する。

1998年3月1日から1998年3月31日の期間には、バージョン3である配送用鍵K dが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ5 1で利用される。

1998年4月1日における、EMDサービスセンタ1の配送用鍵K dのコンテンツプロバイダ2、およびレシーバ5 1への送信を図7で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年4月から1998年9月まで利用可能な、バージョン4乃至バージョン9の6つの配送用鍵K dを送信し、コンテンツプロバイダ2は、6つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、レシーバ5 1に、1998年4月から1998年6月まで、利用可能なバージョン3乃至バージョン5である3つの配送用鍵K dを送信し、レシーバ5 1は、3つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵K d、バージョン2である配送用鍵K d、およびバージョン3である配送用鍵K dをそのまま記憶する。

1998年4月1日から1998年4月30日の期間には、バージョン4である配送用鍵K dが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ5 1で利用される。

このように、あらかじめ先の月の配送用鍵K dを配布しておくことで、仮にユーザが1, 2ヶ月まったくEMDサービスセンタ1にアクセスしていなくても、一応、コンテンツの買い取りが行え、時を見計らって、EMDサービスセンタ1にアクセスして鍵を受信することができる。

図3に戻り、経歴データ管理部15は、ユーザ管理部18から出力される、課金情報、そのコンテンツに対応するPT、およびそのコンテンツに対応するUCPなどを記憶する。

利益分配部16は、経歴データ管理部15から供給された各種情報に基づき、EMDサービスセンタ1、コンテンツプロバイダ2、およびサービスプロバイダ3の利益をそれぞれ算出し、その結果をサービスプロバイダ管理部11、コンテンツプロバイダ管理部12、出納部20、および著作権管理部13に出力する。

相互認証部17は、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の機器と相互認証を実行する。ユーザ管理部18は、所定の処理に対応して登録リスト（後述）を作成し、配送用鍵Kdとともにユーザホームネットワーク5に送信する。

課金請求部19は、経歴データ管理部15から供給された、例えば、課金情報、UCP、およびPTに基づき、ユーザへの課金を算出し、その結果を、出納部20に供給する。出納部20は、ユーザ、コンテンツプロバイダ2、およびサービスプロバイダ3への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。出納部20はまた、決算処理の結果をユーザ管理部18に通知する。

監査部21は、ユーザホームネットワーク5の機器から供給された課金情報、PT、およびUCPの正当性（すなわち、不正をしていないか）を監査する。なお、この場合、EMDサービスセンタ1は、コンテンツプロバイダ2からのUCPを、サービスプロバイダ3からのPTを、そしてユーザホームネットワーク5からのUCPとPTを、それぞれ受け取る。

### （3）コンテンツプロバイダ

図8は、コンテンツプロバイダ2の機能的構成を示すブロック図である。コンテンツサーバ31は、ユーザに供給するコンテンツを記憶し、ウォーターマーク付加部32に供給する。ウォーターマーク付加部32は、コンテンツサーバ31から供給されたコンテンツにウォーターマーク（電子透かし）を付加し、圧縮部33に

供給する。

圧縮部 33 は、ウォーターマーク付加部 32 から供給されたコンテンツを、A T R A C 2 (A d a p t i v e T r a n s f o r m A c o u s t i c C o d i n g 2) (商標) 等の方式で圧縮し、暗号化部 34 に供給する。暗号化部 34 は、圧縮部 33 で圧縮されたコンテンツを、乱数発生部 35 から供給された乱数を鍵 (以下、この乱数をコンテンツ鍵  $K_{co}$  と称する) として、D E S (D a t a E n c r y p t i o n S t a n d a r d) などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部 38 に出力する。

乱数発生部 35 は、コンテンツ鍵  $K_{co}$  となる所定のビット数の乱数を暗号化部 34 および暗号化部 36 に供給する。暗号化部 36 は、コンテンツ鍵  $K_{co}$  を E M D サービスセンタ 1 から供給された配送用鍵  $K_d$  を使用して、D E S などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部 38 に出力する。

D E S は、56 ビットの共通鍵を用い、平文の 64 ビットを 1 ブロックとして処理する暗号方式である。D E S の処理は、平文を攪拌し、暗号文に変換する部分 (データ攪拌部) と、データ攪拌部で使用する鍵 (拡大鍵) を共通鍵から生成する部分 (鍵処理部) からなる。D E S のすべてのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

まず、平文の 64 ビットは、上位 32 ビットの  $H_0$ 、および下位 32 ビットの  $L_0$  に分割される。鍵処理部から供給された 48 ビットの拡大鍵  $K_1$ 、および下位 32 ビットの  $L_0$  を入力とし、下位 32 ビットの  $L_0$  を攪拌した F 関数の出力が算出される。F 関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の 2 種類の基本変換から構成されている。次に、上位 32 ビットの  $H_0$  と、F 関数の出力が排他的論理和され、その結果は  $L_1$  とされる。 $L_0$  は、 $H_1$  とされる。

上位 32 ビットの  $H_0$  および下位 32 ビットの  $L_0$  を基に、以上の処理を 16 回繰り返し、得られた上位 32 ビットの  $H_{16}$  および下位 32 ビットの  $L_{16}$  が暗号文

として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

ポリシー記憶部 37 は、コンテンツに対応して設定される UCP を記憶し、セキュアコンテンツ作成部 38 に出力する。図 9 は、コンテンツサーバ 31 に保持されているコンテンツ A に対応して設定され、ポリシー記憶部 37 に記憶されている UCP A、B を表している。UCP は、「コンテンツの ID」、「コンテンツプロバイダの ID」、「UCP の ID」、「UCP の有効期限」、「利用条件」、「利用内容」の各項目に対応する所定の情報が含まれる。「コンテンツの ID」には、UCP が対応するコンテンツの ID が設定される。UCP A (図 9 A) および UCP B (図 9 B) のそれぞれの「コンテンツの ID」には、コンテンツ A の ID が設定されている。

「コンテンツプロバイダの ID」には、コンテンツの提供元のコンテンツプロバイダの ID が設定される。UCP A および UCP B のそれぞれの「コンテンツプロバイダの ID」には、コンテンツプロバイダ 2 の ID が設定されている。「UCP の ID」には、各 UCP に割り当てられた所定の ID が設定され、UCP A の「UCP の ID」には、UCP A の ID が、UCP B の「UCP の ID」には、UCP B の ID が、それぞれ設定されている。「UCP の有効期限」には、UCP の有効期限を示す情報が設定され、UCP A の「UCP の有効期限」には、UCP A の有効期限が、UCP B の「UCP の有効期限」には、UCP B の有効期限が、それぞれ設定されている。

「利用条件」には、「ユーザ条件」および「機器条件」の各項目に対応する所定の情報が設定され、「ユーザ条件」には、この UCP を選択することができるユーザの条件が設定され、「機器条件」には、この UCP を選択することができる機器の条件が設定されている。

UCP A の場合、「利用条件 10」が設定され、「利用条件 10」の「ユーザ条件 10」には、所定の利用ポイントが 200 ポイント以上が条件であることを示す情報(“200 ポイント以上”)が設定されている。また「利用条件 10」の「

機器条件 10」には、条件がないことを示す情報（”条件なし”）が設定されている。すなわち、UCPAは、200ポイント以上の利用ポイントを有するユーザのみが選択可能となる。

UCPBの場合、「利用条件 20」が設定され、「利用条件 20」の「ユーザ条件 20」には、所定の利用ポイントが200ポイントより少ないことが条件であることを示す情報（“200ポイントより少ない”）が設定されている。また「利用条件 20」の「機器条件 20」には、“条件なし”が設定されている。すなわち、UCPBは、200ポイントより少ない利用ポイントを有するユーザのみが選択可能となる。

「利用内容」には、「ID」、「形式」、「パラメータ」、および「管理移動許可情報」の各項目に対応する所定の情報が含まれる。「ID」には、「利用内容」に設定される情報に割り当てられた所定のIDが設定される。「形式」には、再生や複製など、コンテンツの利用形式を示す情報が設定される。「パラメータ」には、「形式」に設定された利用形式に対応する所定の情報が設定される。

「管理移動許可情報」には、コンテンツの管理移動が可能か否か（許可されているか否かを示す情報（“可”または“不可”））が設定される。コンテンツの管理移動が行われると、図10Aに示すように、管理移動元の機器にコンテンツが保持されつつ、管理移動先の機器にそのコンテンツが移動される。すなわち、管理移動元の機器と管理移動先の機器の両方において、コンテンツが利用される。この点で、図10Bに示すように、移動元の機器にコンテンツが保持されず、移動先の機器のみにコンテンツが保持され、移動先の機器においてのみコンテンツが利用される、通常の移動とは異なる。

また、コンテンツの管理移動が行われている間、管理移動元の機器は、図10Aに示すように、他の機器にコンテンツを管理移動することができない（許可されていない）。すなわち、管理移動元の機器と管理移動先の機器の2機においてのみコンテンツが保持される。この点で、図11Aに示すように、オリジナルのコンテンツから、複数の複製（第1世代）を作成することができる、第1世代の

複製とも異なる。また、管理移動元の機器からコンテンツを戻すことより、他の機器にコンテンツを管理移動することができるので、この点で、図 1 1 B に示すように、1 回だけの複製とも異なる。

図 9 A に戻り、U C P A には、4 つの「利用内容 1 1」乃至「利用内容 1 4」が設けられており、「利用内容 1 1」において、その「I D 1 1」には、「利用内容 1 1」に割り当てられた所定の I D が設定されている。「形式 1 1」には、コンテンツを買い取って再生する利用形式を示す情報（“買い取り再生”）が設定され、「パラメータ 1 1」には、“買い取り再生”に対応する所定の情報が設定されている。「管理移動許可情報 1 1」には、コンテンツの管理移動が許可されていることを示す情報（“可”）が設定されている。

「利用内容 1 2」において、その「I D 1 2」には、「利用内容 1 2」に割り当てられた所定の I D が設定されている。「形式 1 2」には、第 1 世代の複製を行う利用形式を示す情報（“第 1 世代複製”）が設定されている。第 1 世代複製は、図 1 1 A に示したように、オリジナルのコンテンツから、複数の第 1 世代の複製を作成することができる。ただし、第 1 世代の複製から第 2 世代の複製を作成することはできない（許可されていない）。「パラメータ 1 2」には、“第 1 世代複製”に対応する所定の情報が設定されている。「管理移動許可情報 1 2」には、コンテンツの管理移動が許可されていないことを示す情報（“不可”）が設定されている。

「利用内容 1 3」において、その「I D 1 3」には、「利用内容 1 3」に割り当てられた所定の I D が設定されている。「形式 1 3」には、所定の期間（時間）に限って再生する利用形式を示す情報（“期間制限再生”）が設定され、「パラメータ 1 3」には、“期間制限再生”に対応して、その期間の開始時期（時刻）と終了時期（時刻）が設定されている。「管理移動許可情報 1 3」には、“不可”が設定されている。

「利用内容 1 4」において、その「I D 1 4」には、「利用内容 1 4」に割り当てられた所定の I D が設定されている。「形式 1 4」には、5 回の複製を行う

利用形式を示す情報 (“Pay Per Copy 5”) が設定されている。なお、この場合も、図 11 の B に示すように、複製からの複製を作成することはできない (許可されていない)。「パラメータ 14」には、複製が 5 回可能であることを示す情報 (“複製 5 回”) が設定されている。「管理移動許可情報 14」には、“不可” が設定されている。

図 9 B の UCPB には、2 つの「利用内容 21」、および「利用内容 22」が設けられている。「利用内容 21」において、その「ID 21」には、「利用内容 21」に割り当てられた所定の ID が設定されている。「形式 21」には、4 回の再生を行う利用形式を示す情報 (“Pay Per Play 4”) が設定され、「パラメータ 21」には、再生が 4 回可能であることを示す情報 “再生 4 回” が設定されている。「管理移動許可情報 21」には、“不可” が設定されている。

「利用内容 22」において、その「ID 22」には、「利用内容 22」に割り当てられた所定の ID が設定されている。「形式 22」には、“Pay Per Copy 2” が設定され、「パラメータ 22」には、“複製 2 回” が設定されている。「管理移動許可情報 22」には、“不可” が設定されている。

ここで、UCPA および UCPB の内容を比較すると、200 ポイント以上の利用ポイントを有するユーザは、4 通りの利用内容 11 乃至利用内容 14 から利用内容を選択することができるのに対して、200 ポイントより少ない利用ポイントを有するユーザは、2 通りの利用内容 21, 22 からしか利用内容を選択することができないものとされている。

ところで、図 9 は、UCPA および UCPB を模擬的に表しているが、例えば、UCPA の「利用条件 10」および UCPB の「利用条件 20」には、実際は、図 12 A に示すサービスコード、および図 12 B に示すコンディションコードの他、サービスコードに対応して数値や所定の種類を示すバリューコードがそれぞれ設定されている。

図 13 A は、UCPA (図 9 A) の「利用条件 10」の「ユーザ条件 10」および「機器条件 10」として設定されている各コードのコード値を表している。

UCPAの「利用条件10」の「ユーザ条件10」は、“200ポイント以上”とされているので、“利用ポイントに関し条件有り”を意味する80xxhのサービスコード(図12A)が、このとき数値200を示す0000C8hのバリューコードが、そして“>= (以上)”を意味する06hのコンディションコード(図12B)が、ユーザ条件として設定されている。

UCPAの「機器条件10」は、“条件なし”とされているので、“条件なし”を意味する0000hのサービスコード(図12A)が、このとき何ら意味を持たないFFFFFFhのバリューコードが、そして”無条件”を意味する00hのコンディションコード(図12B)が、機器条件として設定されている。

図13Bは、UCPBの「利用条件20」の「ユーザ条件20」および「機器条件20」として設定されている各コードのコード値を表している。「ユーザ条件20」は、“200ポイントより少ない”とされているので、“利用ポイントに関し条件有り”を意味する80xxhのサービスコード(図12A)が、数値200を示す0000C8hのバリューコードが、そして“< (より小さい)”を意味する03hのコンディションコード(図12B)が、ユーザ条件として設定されている。

UCPBの「機器条件20」は、UCPAの「機器条件10」と同様に、“条件なし”とされ、同一のコード値が設定されているので、その説明は省略する。

図8に戻り、セキュアコンテナ作成部38は、例えば、図14に示すような、コンテンツA(コンテンツ鍵KcoAで暗号化されている)、コンテンツ鍵KcoA(配送用鍵Kdで暗号化されている)、UCPA、B、および署名からなるコンテンツプロバイダセキュアコンテナを作成する。なお、署名は、送信したいデータ(この場合、コンテンツA(コンテンツ鍵KcoAで暗号化されている))、コンテンツ鍵KcoA(配送用鍵Kdで暗号化されている)、およびUCPA、Bの全体にハッシュ関数を適用して得られたハッシュ値が、コンテンツプロバイダの公開鍵暗号の秘密鍵(この場合、コンテンツプロバイダ2の秘密鍵Kscp)で暗号化されたものである。

セキュアコンテナ作成部 38 はまた、コンテンツプロバイダセキュアコンテナに、図 15 に示すコンテンツプロバイダ 2 の証明書を付してサービスプロバイダ 3 に送信する。この証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ 2 に対し割り付けた証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、およびコンテンツプロバイダ 2 の名前、コンテンツプロバイダ 2 の公開鍵  $K_{p\ c\ p}$ 、並びにその署名（認証局の秘密鍵  $K_{s\ c\ a}$  で暗号化されている）から構成されている。

署名は、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵で暗号化して作成される。

ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの 1 ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、MD (Message Digest) 4, MD5, SHA (Secure Hash Algorithm) - 1 などが用いられる。

次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を

秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

公開鍵暗号の中で代表的なRSA (Rivest-Shamir-Adleman) 暗号を、簡単に説明する。まず、2つの十分に大きな素数である  $p$  および  $q$  を求め、さらに  $p$  と  $q$  の積である  $n$  を求める。 $(p-1)$  と  $(q-1)$  の最小公倍数  $L$  を算出し、更に、3以上  $L$  未満で、かつ、 $L$  と互いに素な数  $e$  を求める (すなわち、 $e$  と  $L$  を共通に割り切れる数は、1のみである)。

次に、 $L$  を法とする乗算に関する  $e$  の乗法逆元  $d$  を求める。すなわち、 $d$ 、 $e$ 、および  $L$  の間には、 $ed = 1 \pmod{L}$  が成立し、 $d$  はユークリッドの互除法で算出できる。このとき、 $n$  と  $e$  が公開鍵とされ、 $p$ 、 $q$ 、および  $d$  が、秘密鍵とされる。

暗号文  $C$  は、平文  $M$  から、式 (1) の処理で算出される。

$$C = M^e \pmod{n} \quad \dots\dots (1)$$

暗号文  $C$  は、式 (2) の処理で平文  $M$  に、復号される。

$$M = C^d \pmod{n} \quad \dots\dots (2)$$

証明は省略するが、RSA暗号で平文を暗号文に変換して、それが復号できるのは、フェルマーの小定理に根拠をおいており、式 (3) が成立するからである。

$$M = C^d = (M^e)^d = M^{ed} = M \pmod{n} \quad \dots\dots (3)$$

秘密鍵  $p$  と  $q$  を知っているならば、公開鍵  $e$  から秘密鍵  $d$  は算出できるが、公開鍵  $n$  の素因数分解が計算量的に困難な程度に公開鍵  $n$  の桁数を大きくすれ

ば、公開鍵  $n$  を知るだけでは、公開鍵  $e$  から秘密鍵  $d$  は計算できず、復号できない。以上のように、RSA暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

また、公開鍵暗号の他の例である楕円曲線暗号 (Elliptic Curve Cryptography) についても、簡単に説明する。楕円曲線  $y^2 = x^3 + ax + b$  上の、ある点を  $B$  とする。楕円曲線上の点の加算を定義し、 $nB$  は、 $B$  を  $n$  回加算した結果を表す。同様に、減算も定義する。 $B$  と  $nB$  から  $n$  を算出することは、困難であることが証明されている。 $B$  と  $nB$  を公開鍵とし、 $n$  を秘密鍵とする。乱数  $r$  を用いて、暗号文  $C1$  および  $C2$  は、平文  $M$  から、公開鍵で式 (4) および式 (5) の処理で算出される。

$$C1 = M + r n B \quad \dots\dots (4)$$

$$C2 = r B \quad \dots\dots (5)$$

暗号文  $C1$  および  $C2$  は、式 (6) の処理で平文  $M$  に、復号される。

$$M = C1 - n C2 \quad \dots\dots (6)$$

復号できるのは、秘密鍵  $n$  を有するものだけである。以上のように、RSA暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

図8に、再び戻り、コンテンツプロバイダ2の相互認証部39は、EMDサービスセンタ1から配送用鍵  $Kd$  の供給を受けるのに先立ち、EMDサービスセンタ1と相互認証する。また相互認証部39は、サービスプロバイダ3へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ3と相互認証することも可能であるが、この例の場合、コンテンツプロバイダセキュアコンテナには、秘密しなければならない情報が含まれていないので、この相互認証

は必ずしも必要とされるわけではない。

#### (4) サービスプロバイダ

次に、図16のブロック図を参照して、サービスプロバイダ3の機能的構成を説明する。コンテンツサーバ41は、コンテンツプロバイダ2から供給されたコンテンツプロバイダセキュアコンテナに含まれる、コンテンツ(コンテンツ鍵K<sub>co</sub>で暗号化されている)、コンテンツ鍵K<sub>co</sub>(配送用鍵K<sub>d</sub>で暗号化されている)、UCP、およびコンテンツプロバイダ2の署名を記憶し、セキュアコンテナ作成部44に供給する。

値付け部42は、コンテンツプロバイダ2から供給されたコンテンツプロバイダセキュアコンテナに含まれる署名に基づいて、コンテンツプロバイダセキュアコンテナの正当性を検証するが、この場合、コンテンツプロバイダ2の証明書が検証され、正当であるとき、コンテンツプロバイダ2の公開鍵が取得される。そしてこの取得された公開鍵に基づいて、コンテンツプロバイダセキュアコンテナの正当性が検証される。

コンテンツプロバイダセキュアコンテナの正当性を確認すると、値付け部42は、コンテンツプロバイダセキュアコンテナに含まれるUCPに対応する、PTを作成し、セキュアコンテナ作成部44に供給する。図17は、図9AのUCP Aに対応して作成された、2つのPTA-1(図17A)およびPTA-2(図17B)を表している。PTには、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「価格条件」、および「価格内容」の各項目に対応する所定の情報が含まれる。

PTの、「コンテンツのID」、「コンテンツプロバイダのID」、および「UCPのID」の各項目には、UCPの、これらに対応する項目の情報が、それぞれ設定される。すなわち、PTA-1およびPTA-2のそれぞれの「コンテンツのID」には、コンテンツAのIDが、それぞれの「コンテンツプロバイダのID」には、コンテンツプロバイダ2のIDが、そしてそれぞれの「UCPのID

」には、UCPAのIDが設定されている。

「サービスプロバイダのID」には、PTの提供元のサービスプロバイダ2のIDが設定される。PTA-1およびPTA-2のそれぞれの「サービスプロバイダのID」には、サービスプロバイダ3のIDが設定されている。「PTのID」には、各PTに割り当てられた所定のIDが設定される。PTA-1の「PTのID」には、PTA-1のIDが、PTA-2の「PTのID」には、PTA-2のIDがそれぞれ設定されている。「PTの有効期限」には、PTの有効期限を示す情報が設定される。PTA-1の「PTの有効期限」には、PTA-1の有効期限が、PTA-2の「PTの有効期限」には、PTA-2の有効期限が設定されている。

「価格条件」には、UCPの「利用条件」と同様に、「ユーザ条件」および「機器条件」の各項目に対応する所定の情報が設定されている。「価格条件」の「ユーザ条件」には、このPTを選択することができるユーザの条件を示す情報が設定され、その「機器条件」には、このPTを選択することができる機器の条件を示す情報が設定される。

PTA-1の場合、「価格条件10」が設定され、「価格条件10」の「ユーザ条件10」には、ユーザが男性であることを示す情報（“男性”）が設定され、その「機器条件10」には、“条件なし”が設定されている。すなわち、PTA-1は、男性のユーザのみが選択可能となる。

PTA-1の「価格条件10」の「ユーザ条件10」および「機器条件10」も、実際は、図18Aに示すように、各種コードのコード値が設定されている。「価格条件10」の「ユーザ条件10」には、“性別条件有り”を意味する01xxhのサービスコード（図12A）が、このとき男性を意味する000000hのバリューコードが、そして“=”を意味する01hのコンディションコード（図12B）が設定されている。「機器条件10」には、“条件なし”を意味する0000hのサービスコードが、この場合何ら意味を持たないFFFFFFhのバリューコードが、そして“無条件”を意味する00hのコンディションコード

が設定されている。

P T A - 2 の場合、「価格条件 2 0」が設定され、「価格条件 2 0」の「ユーザ条件 2 0」には、ユーザが女性であることを示す情報（“女性”）が設定され、その「機器条件 2 0」には、“条件なし”が設定されている。すなわち、P T A - 2 は、女性のユーザのみが選択可能となる。

P T A - 2 の「価格条件 2 0」の「ユーザ条件 2 0」および「機器条件 2 0」も、実際は、図 1 8 B に示すように、各コードのコード値が設定されている。「価格条件 2 0」の「ユーザ条件 2 0」には、“性別条件有り”を意味する 0 1 x x h のサービスコード（図 1 2 A）が、この場合女性を示す 0 0 0 0 0 1 h のバリューコードが、そして“=”を意味する 0 1 h のコンディションコード（図 1 2 B）が設定されている。その「機器条件 2 0」には、“条件なし”を意味する 0 0 0 0 h のサービスコードが、この場合何ら意味を持たない F F F F F F h のバリューコードが、そして“無条件”を意味する 0 0 h のコンディションコードが設定されている。

図 1 7 に戻り、P T の「価格内容」には、対応する U C P の「利用内容」の「形式」に設定されている利用形式の利用料金が示されている。すなわち、P T A - 1 の「価格内容 1 1」に設定された“2 0 0 0 円”および P T A - 2 の「価格内容 2 1」に設定された“1 0 0 0 円”は、U C P A（図 9 A）の「利用内容 1 1」の「形式 1 1」が“買い取り再生”とされているので、コンテンツ A の買い取り価格（料金）を示している。

P T A - 1 の「価格内容 1 2」の“6 0 0 円”および P T A - 2 の「価格内容 2 2」の“3 0 0 円”は、U C P A の「利用内容 1 2」の「形式 1 2」より、第 1 世代複製の利用形式でコンテンツ A を利用する場合の料金を示している。P T A - 1 の「価格内容 1 3」の“1 0 0 円”および P T A - 2 の「価格内容 2 3」の“5 0 円”は、U C P A の「利用内容 1 3」の「形式 1 3」より、期間制限再生の利用形式でコンテンツ A を利用する場合の料金を示している。P T A - 1 の「価格内容 1 4」の“3 0 0 円”および P T A - 2 の「価格内容 2 4」の“1 5

0円”は、UCPAの「利用内容14」の「形式14」より、5回の複製を行う利用形式でコンテンツAを利用する場合の料金を示している。

なお、この例の場合、PTA-1（男性ユーザに適用される）の価格内容と、PTA-2（女性ユーザに適用される）の価格内容を比較すると、PTA-1の価格内容に示される価格が、PTA-2の価格内容に示される価格の2倍に設定されている。例えば、UCPAの「利用内容11」に対応するPTA-1の「価格内容11」が“2000円”とされているのに対し、同様にUCPAの「利用内容11」に対応するPTA-2の「価格内容21」は“1000円”とされている。同様に、PTA-1の「価格内容12」乃至「価格内容14」に設定されている価格は、PTA-2の「価格内容22」乃至「価格内容24」に設定されている価格に2倍とされている。すなわち、この例の場合、コンテンツAは、女性のユーザがより低価格で利用できるコンテンツとされている。

図19は、図9BのUCPBに対応して作成された、2つのPTB-1およびPTB-2を表している。図19AのPTB-1には、コンテンツAのID、コンテンツプロバイダ2のID、UCPBのID、UCPBの有効期限、サービスプロバイダ3のID、PTB-1のID、PTB-1の有効期限、価格条件30、2通りの価格内容31、32などが含まれている。

PTB-1の「価格条件30」の「ユーザ条件30」には“条件なし”が設定され、「機器条件30」には、機器が従機器であることを条件とする情報（“従機器”）が設定されている。すなわち、PTB-1は、コンテンツAが従機器において利用される場合にのみ選択可能となる。なお、従機器とは、自分自身が、所定のコンテンツを購入するための処理や、課金を決済する処理などを行うことができない機器を意味する。

PTB-1の「価格条件30」の「ユーザ条件30」および「機器条件30」にも、実際は、図20Aに示すように、各コードのコード値が設定されている。「ユーザ条件30」には、“条件なし”を意味する0000hのサービスコード（図12A）が、この場合何ら意味を持たないFFFFFFhのバリューコード

が、そして“無条件”を意味する00hのコンディションコード（図12B）が設定されている。「機器条件30」は、“従機器”とされているので、“機器に関し条件有り”を意味する00xxhのサービスコードが、このとき“数値100”を示す000064hのバリューコードが、そして“<（小さい）”を意味する03hのコンディションコードが設定されている。この例の場合、従機器には、100番より小さい機器番号が設定されているので、このようなコード値が設定される。

PTB-1の「価格内容31」の“100円”は、UCPB（図9B）の「利用内容21」の「形式21」が“Pay Per Play 4”とされているので、4回の再生を行う場合の料金を示し、「価格内容32」の“300円”は、UCPBの「利用内容22」の「形式22」が“Pay Per Copy 2”とされているので、2回の複製を行う場合の料金を示している。

UCPBに対応して作成された、もう一方のPTB-2には、図19Bに示すように、コンテンツAのID、コンテンツプロバイダ2のID、UCPBのID、UCPB、サービスプロバイダ3のID、PTB-2のID、PTB-2の有効期限、価格条件40、および2通りの価格内容41、42などが含まれている。

PTB-2の「価格条件40」の「ユーザ条件40」には“条件なし”が設定され、その「機器条件40」には、機器が主機器であることを条件とする情報（“主機器”）が設定されている。すなわち、PTB-2は、主機器においてコンテンツが利用される場合にのみ選択可能となる。なお、主機器とは、自分自身が、所定のコンテンツを購入するための処理や、課金を決済する処理などを行うことができる機器を意味する。

PTB-2の「価格条件40」の「ユーザ条件40」および「機器条件40」にも、実際は、図20Bに示すように、各コードのコード値が設定されている。「価格条件40」の「ユーザ条件40」には、“条件なし”を意味する0000hのサービスコード（図12A）が、この場合何ら意味を持たないFFFFFF

hのバリューコードが、そして”無条件”を意味する00hのコンディションコード(15B)が設定されている。「機器条件40」には、“機器に関し条件有り”を意味する00xxhのサービスコードが、このとき“数値100”を示す000064hのバリューコードが、そして“=>(以上)”を意味する06hのコンディションコードが設定されている。この例の場合、主機器には、100番以上の機器番号が設定されているので、このようなコード値が設定される。

PTB-2の「価格内容41」および「価格内容42」のそれぞれに示される価格は、UCPBの「利用内容21」の「形式21」および「利用内容22」の「形式22」のそれぞれに示される利用形式でコンテンツAを利用する場合の料金を示している。

ここで、PTB-1(従機器に適用される)の価格内容とPTB-2(主機器に適用される)の価格内容を比較すると、PTB-1の価格内容は、PTB-2の価格内容の2倍に設定されている。例えば、PTB-1の「価格内容31」が“100円”とされているのに対し、PTB-2の「価格内容41」は50円とされており、「価格内容32」が“300円”とされているのに対して、「価格内容42」は“150円”とされている。

図16に戻り、ポリシー記憶部43は、コンテンツプロバイダ2から供給された、コンテンツのUCPを記憶し、セキュアコンテナ作成部44に供給する。

セキュアコンテナ作成部44は、例えば、図21に示すような、コンテンツA(コンテンツ鍵KcoAで暗号化されている)、コンテンツ鍵KcoA(配送用鍵Kdで暗号化されている)、UCPA, B、コンテンツプロバイダ2の署名、PTA-1, A-2, B-1, B-2、およびサービスプロバイダ3の署名からなるサービスプロバイダセキュアコンテナを作成する。

セキュアコンテナ作成部44はまた、作成したサービスプロバイダセキュアコンテナを、図22に示すような、証明書のバージョン番号、認証局がサービスプロバイダ3に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ3の名前

、サービスプロバイダ3の公開鍵 $K_{psp}$ 、並びに認証局の署名より構成されるサービスプロバイダの証明書を付して、ユーザホームネットワーク5に供給する。

図16に、再び戻り、相互認証部45は、コンテンツプロバイダ2からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロバイダ2と相互認証する。相互認証部45また、ユーザホームネットワーク5へのサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク5と相互認証するが、このサービスプロバイダ3とユーザホームネットワーク5との相互認証は、例えば、ネットワーク4が衛星通信である場合、実行されない。なお、この例の場合、コンテンツプロバイダセキュアコンテナおよびサービスプロバイダセキュアコンテナには、特に、秘密情報が含まれていないので、サービスプロバイダ3は、コンテンツプロバイダ2およびユーザホームネットワーク5と相互認証を行わなくてもよい。

#### (5) ユーザホームネットワーク

##### (5-1) レシーバ51

図23は、ユーザホームネットワーク5を構成するレシーバ51の構成例を表している。レシーバ51は、通信部61、SAM (Secure Application Module) 62、外部記憶部63、伸張部64、通信部65、インタフェース66、表示制御部67、および入力制御部68より構成される、HDD52に接続される据え置き型の機器である。

レシーバ51の通信部61は、ネットワーク4を介してサービスプロバイダ3、またはEMDサービスセンタ1と通信し、所定の情報を受信し、または送信する。

SAM62は、相互認証モジュール71、課金処理モジュール72、記憶モジュール73、復号/暗号化モジュール74、およびデータ検査モジュール75からなるが、シングルチップの暗号処理専用ICで構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電

圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパー性）を有している。

SAM 62の相互認証モジュール71は、記憶モジュール73に記憶されている、図24に示すSAM 62の証明書を、相互認証相手に送信し、相互認証を実行し、これにより、認証相手と共有することとなった一時鍵Ktemp（セッション鍵）を復号／暗号化モジュール74に供給する。SAMの証明書には、コンテンツプロバイダ2の証明書（図15）およびサービスプロバイダ3の証明書（図22）に含まれている情報に対応する情報が含まれているので、その説明は省略する。

課金処理モジュール72は、選択されたUCPの利用内容に基づいて、使用許諾条件情報UCSおよび課金情報を作成する。図25は、コンテンツが“買い取り再生”の利用形式で権利購入された場合のUCSの例であり、図9Aに示したUCPAの利用内容11と、図17Aに示したPTA-1の価格内容11に基づいて作成されたUCSAを表している。UCSには、図25に示されるように、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、「利用内容」、および「利用履歴」の各項目に対応する所定の情報が設定される。

UCSの、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、および「PTの有効期限」の各項目には、PTの、それらに対応する項目の情報が設定される。すなわち、図25のUCSAの、「コンテンツのID」には、コンテンツAのIDが、「コンテンツプロバイダのID」には、コンテンツプロバイダ2のIDが、「UCPのID」には、UCPAのIDが、「UCPの有効期限」には、UCPAの有効期限が、「サービスプロバイダのID」には、サービスプロバイダ3のIDが、「PTのID」には、PTA-1のIDが、そして「PTの有効期限」には、PTA-1の有効期限が、それぞれ設定されている。

「UCSのID」には、UCSに割り当てられた所定のIDが設定され、UCSAの「UCSのID」には、UCSAのIDが設定されている。「SAMのID」には、機器のSAMのIDが設定され、UCSAの「SAMのID」には、レシーバ51のSAM62のIDが設定されている。「ユーザのID」には、コンテンツを利用するユーザのIDが設定され、UCSAの「ユーザのID」には、レシーバ51のユーザのIDが設定されている。

「利用内容」は、「ID」、「形式」、「パラメータ」、および「管理移動状態情報」の各項目からなり、そのうち「ID」、「形式」、および「パラメータ」の項目には、選択されたUCPの「利用内容」の、それらに対応する項目の情報が設定される。すなわち、UCSAの「ID」には、UCPAの「利用内容11」の「ID11」に設定されている情報（利用内容11のID）が、「形式」には、「利用内容11」の「形式11」に設定されている“買い取り再生”が、「パラメータ」には、「利用内容11」の「パラメータ11」に設定されている情報（“買い取り再生”に対応する情報）が設定されている。

「利用内容」の「管理移動状態情報」には、選択されたUCPの「管理移動許可情報」に“可”が設定されている場合（管理移動が行える場合）、管理移動元の機器（コンテンツを購入した機器）と管理移動先の機器のそれぞれのIDが設定されるようになされている。なお、コンテンツの管理移動が行われていない状態においては、管理移動元の機器のIDが、管理移動先の機器のIDとしても設定される。一方、UCPの「管理移動許可情報」に、“不可”が設定されている場合、「管理移動状態情報」には“不可”が設定される。すなわち、この場合、コンテンツの管理移動は行われな（許可されない）。UCSAの「管理移動状態情報」には、UCPAの「利用内容11」の「管理移動許可情報11」に“可”が設定されており、また、このとき、コンテンツAは管理移動されていないので、SAM62のIDが、管理移動元の機器のIDおよび管理移動先の機器のIDとして設定されている。

「利用履歴」には、同一のコンテンツに対する利用形式の履歴が設定される。

UCSAの「利用履歴」には、「買い取り再生」を示す情報のみが記憶されているが、例えば、レシーバ51において、コンテンツAが以前に利用されていた場合、そのときの利用形式も記憶される。

なお、上述したUCSにおいては、「UCPの有効期限」および「PTの有効期限」が設けられているがそれらをUCSに設定しないようにすることもできる。また、上述したUCSにおいて、「コンテンツプロバイダのID」が設けられているが、UCPのIDがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのID」も同様に、PTのIDがユニークで、これにより、サービスプロバイダを特定することができる場合、それを設けないようにすることもできる。

作成されたUCSは、レシーバ51の復号／暗号化モジュール74の復号化ユニット91から供給されるコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）とともに、外部記憶部63に送信され、その利用情報記憶部63Aに記憶される。外部記憶部63の利用情報記憶部63Aは、図26に示すように、M個のブロックBP-1乃至BP-Mに分割され（例えば、1メガバイト毎に分割され）、各ブロックBPが、N個の利用情報用メモリ領域RP-1乃至RP-Nに分割されている。SAM62から供給されるコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）およびUCSは、利用情報用記憶部63Aの所定のブロックBPの利用情報用メモリ領域RPに、対応して記憶される。

図26の例では、ブロックBP-1の利用情報用メモリ領域RP-3に、図25に示したUCSAとコンテンツ鍵KcoA（保存用鍵Ksaveで暗号化されている）が対応して記憶されている。ブロックBP-1の利用情報用メモリ領域RP-1，RP-2には、他のコンテンツ鍵Kco1，Kco2（それぞれ保存用鍵Ksaveで暗号化されている）およびUCS1，2がそれぞれ記憶されている。ブロックBP-1の利用情報用メモリ領域RP-4（図示せず）乃至RP-N、およびブロックBP-2（図示せず）乃至BP-Mには、この場合、コン

テンツ鍵K c oおよびU C Sは記憶されておらず、空いていることを示す所定の初期情報が記憶されている。なお、利用情報用メモリ領域R Pに記憶されるコンテンツ鍵K c o（保存用鍵K s a v eで暗号化されている）およびU C Sを、個々に区別する必要がない場合、まとめて、利用情報と称する。

図27は、図25に示したU C S Aと同時に作成された課金情報Aを表している。課金情報は、図27に示されるように、「コンテンツのID」、「コンテンツプロバイダのID」、「U C PのID」、「U C Pの有効期限」、「サービスプロバイダのID」、「P TのID」、「P Tの有効期限」、「U C SのID」、「S A MのID」、「ユーザのID」、「利用内容」、および「課金履歴」の各項目に対応する所定の情報が設定される。

課金情報の、「コンテンツのID」、「コンテンツプロバイダのID」、「U C PのID」、「U C Pの有効期限」、「サービスプロバイダのID」、「P TのID」、「P Tの有効期限」、「U C SのID」、「S A MのID」、「ユーザのID」、および「利用内容」には、U C Sの、それらに対応する項目の情報が、それぞれ設定される。すなわち、図27の課金情報Aの、「コンテンツのID」には、コンテンツAのIDが、「コンテンツプロバイダのID」には、コンテンツプロバイダ2のIDが、「U C PのID」には、U C P AのIDが、「U C Pの有効期限」には、U C P Aの有効期限が、「サービスプロバイダのID」には、サービスプロバイダ3のIDが、「P TのID」には、P T A-1のIDが、「P Tの有効期限」には、P T A-1の有効期限が、「U C SのID」には、U C S AのIDが、「S A MのID」には、S A M 6 2のIDが、「ユーザのID」には、ユーザFのIDが、そして「利用内容」には、U C S Aの「利用内容11」の内容が、それぞれ設定されている。

課金情報の「課金履歴」には、機器において計上された課金の合計額を示す情報が設定される。課金情報Aの「課金履歴」には、レシーバ51において計上された課金の合計額が設定されている。

なお、上述した課金情報においては、「U C Pの有効期限」および「P Tの有効期限」

効期限」が設けられているが、それらを課金情報に設定しないようにすることもできる。また、上述した課金情報においては、「コンテンツプロバイダのID」が設けられているが、UCPのIDがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのID」も同様に、PTのIDがユニークで、これにより、サービスプロバイダを特定することができる場合、それを設けないようにすることもできる。

図23に戻り、記憶モジュール73には、図28に示すように、SAM62の公開鍵Kpu、SAM62の秘密鍵Ksu、EMDサービスセンタ1の公開鍵Kpesc、認証局の公開鍵Kpca、保存用鍵Ksave、3ヶ月分の配送用鍵Kdなどの各種鍵、SAM62の証明書、課金情報、基準情報51、およびM個の検査値HP-1乃至HP-Mなどが記憶されている。

記憶モジュール73に記憶される検査値HP-1は、外部記憶部63の利用情報記憶部63AのブロックBP-1に記憶されているデータの全体にハッシュ関数が適用されて算出されたハッシュ値である。検査値HP-2乃至HP-Mも、検査値HP-1と同様に、外部記憶部63の、対応するブロックBP-2乃至BP-Mのそれぞれに記憶されているデータのハッシュ値である。

図29は、記憶モジュール73に記憶されている基準情報51を表している。基準情報には、「SAMのID」、「機器番号」、「決済ID」、「課金の上限額」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」の各項目に設定される所定情報などが含まれている。

基準情報51には、SAM62のID、SAM62の機器番号(100番)、ユーザの決済ID、ユーザの決済ユーザ情報(ユーザの一般情報(氏名、住所、電話番号、決済機関情報、生年月日、年齢、性別)、ユーザのID、およびユーザのパスワード)、および所定の利用ポイント情報が設定されている。

「課金の上限額」には、機器がEMDシステムに正式登録されている状態と仮登録されている状態で、それぞれ異なる課金の上限額が設定される。基準情報5

1の「課金の上限額」には、レシーバ51が正式登録されているので、正式登録されている状態における課金の上限額を示す情報（”正式登録時の上限額”）が設定されている。

図23に戻り、SAM62の復号／暗号化モジュール74は、復号ユニット91、乱数発生ユニット92、および暗号化ユニット93から構成される。復号ユニット91は、暗号化されたコンテンツ鍵Kcoを配送用鍵Kdで復号し、暗号化ユニット93に出力する。乱数発生ユニット92は、必要に応じて（例えば、相互認証時に）、所定の桁数の乱数を発生し、必要に応じて一時鍵Ktempを生成し、暗号化ユニット93に出力する。

暗号化ユニット93は、復号されたコンテンツ鍵Kcoを、再度、記憶モジュール73に保持されている保存用鍵Ksaveで暗号化する。暗号化されたコンテンツ鍵Kcoは、外部記憶部63に供給される。暗号化ユニット93は、コンテンツ鍵Kcoを伸張部64に送信するとき、コンテンツ鍵Kcoを乱数発生ユニット92で生成した一時鍵Ktempで暗号化する。

データ検査モジュール75は、記憶モジュール73に記憶されている検査値HPと、外部記憶部63の利用情報記憶部63Aの、対応するブロックBPのデータのハッシュ値を比較し、ブロックBPのデータが改竄されていないか否かを検査する。

伸張部64は、相互認証モジュール101、復号モジュール102、復号モジュール103、伸張モジュール104、およびウォーターマーク付加モジュール105から構成される。相互認証モジュール101は、SAM62と相互認証し、一時鍵Ktempを復号モジュール102に出力する。復号モジュール102は、一時鍵Ktempで暗号化されたコンテンツ鍵Kcoを一時鍵Ktempで復号し、復号モジュール103に出力する。復号モジュール103は、HDD52に記録されたコンテンツをコンテンツ鍵Kcoで復号し、伸張モジュール104に出力する。伸張モジュール104は、復号されたコンテンツを、更にATRAC2等の方式で伸張し、ウォーターマーク付加モジュール105に出力する。

。ウォーターマーク付加モジュール105は、コンテンツにレシーバ51を特定するための情報（例えば、SAM62のID）のウォーターマーク（電子透かし）を挿入し、図示せぬスピーカに出力し、音楽を再生する。

通信部65は、ユーザホームネットワーク5のレシーバ201との通信処理を行う。インターフェース66は、SAM62および伸張部64からの信号を所定の形式に変更し、HDD52に出力し、また、HDD52からの信号を所定の形式に変更し、SAM62および伸張部64に出力する。

表示制御部67は、表示部（図示せず）への出力を制御する。入力制御部68は、各種ボタンなどから構成される操作部（図示せず）からの入力を制御する。

HDD52は、サービスプロバイダ3から供給されたコンテンツなどを記憶する他、図30に示すような登録リストを記憶している。この登録リストは、表形式に情報が記憶されているリスト部、および登録リストを保持する機器についての所定の情報が記憶されている対象SAM情報部より構成されている。

対象SAM情報部には、この登録リストを保有する機器のSAM ID、この例の場合、レシーバ51のSAM62のIDが（「対象SAM ID」の欄に）記憶されている。対象SAM情報部にはまた、この登録リストの有効期限が（「有効期限」の欄に）記憶され、登録リストのバージョン番号が（「バージョン番号」の欄に）記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ51には、レシーバ201の1機の機器が接続されているので、自分自身を含む合計値2が（「接続されている機器数」の欄に）記憶されている。

リスト部は、「SAM ID」、「ユーザID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、「状態フラグ」、「公開鍵」、および「署名」の9個の項目から構成され、この例の場合、レシーバ51の登録条件、レシーバ201の登録条件として、それぞれの項目に所定の情報が記憶されている。

「SAM ID」には、機器のSAMのIDが記憶される。この例の場合、レシーバ51のSAM62のID、およびレシーバ201のSAM212のIDが

記憶されている。「ユーザID」には、対応する機器のユーザのユーザIDが記憶される。

「購入処理」には、機器が、コンテンツを購入するための処理を行うことができるか否かを示す情報（“可”または“不可”）が記憶される。この例の場合、レシーバ51およびレシーバ201は、コンテンツを購入するための処理を行うことができるようになされているので、それぞれに対応する「購入処理」には、“可”が記憶されている。

「課金処理」には、機器が、EMDサービスセンタ1との間で、課金処理を行うことができるか否かを示す情報（“可”または“不可”）が記憶される。この例の場合、レシーバ51のみが、課金処理を行うことができ、レシーバ201はその処理を行うことができないようになされているので、レシーバ51に対応する「課金処理」には、“可”が記憶され、レシーバ201に対応する「課金処理」には、“不可”が記憶されている。

「課金機器」には、機器において計上された課金を決済する処理を行う機器のSAMのIDが記憶される。この例の場合、レシーバ51（SAM62）は、自分自身の課金を自分自身で決済することができるので、その対応する「課金機器」には、レシーバ51のSAM62のIDが記憶されている。レシーバ51はまた、自分自身の課金を決済することができないレシーバ201に代わり、その課金を決済するようになされているので、レシーバ201に対応する「課金機器」には、レシーバ51のSAM62のIDが記憶されている。

「コンテンツ供給機器」には、機器が、コンテンツの供給をサービスプロバイダ3からではなく、接続される他の機器から受ける場合、コンテンツを供給することができる機器のSAMのIDが記憶される。この例の場合、レシーバ51およびレシーバ201は、コンテンツの供給をサービスプロバイダ3から受けるので、それぞれに対応する「コンテンツ供給機器」には、コンテンツを供給する機器が存在しない旨を示す情報（“なし”）が記憶されている。

「状態フラグ」には、機器の動作制限条件が記憶される。何ら制限されていな

い場合は、その旨を示す情報（“制限なし”）、一定の制限が課せられている場合は、その旨を示す情報（“制限あり”）、また動作が停止させられている場合には、その旨を示す情報（“停止”）が記憶される。例えば、課金処理が成功しなかった場合、その機器に対応する「状態フラグ」には、“制限あり”が設定される（詳細は後述する）。この例の場合、「状態フラグ」に“制限あり”が設定された機器においては、すでに購入されたコンテンツの再生（解読）処理は実行されるが、新たなコンテンツを購入するための処理は実行されなくなる。すなわち、一定の制限が機器に課せられる。また、コンテンツの不正複製などの違反行為が発覚した場合、「状態フラグ」には、“停止”が設定され、機器の動作が停止される。これにより、その機器はEMDシステムからのサービスを、一切受けることができなくなる。

この例の場合、レシーバ51およびレシーバ201に対しては、何ら制限が課せられていないものとし、それぞれに対応する「状態フラグ」には、“なし”が設定されている。なお、「状態フラグ」に設定される、“制限あり”および“停止”など、動作を制限するための情報を、個々に区別する必要がない場合、まとめて、動作制限情報と称する。

「登録条件署名」には、各登録条件として、それぞれ、「SAMID」、「ユーザID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、および「状態フラグ」に記憶されている情報に対するEMDサービスセンタ1による署名が記憶されている。「登録リスト署名」には、登録リストに設定されているデータの全体に対する署名が記憶されている。

#### （5-2）レシーバ201

図31は、レシーバ201の構成例を表している。レシーバ201の通信部211乃至入力制御部218は、レシーバ51の通信部61乃至入力制御部68と同様の機能を有しているので、その詳細な説明は適宜省略する。

HDD202には、購入したコンテンツの他、図32に示すような、レシーバ201の登録リストが記憶されている。この登録リストの対象SAM情報部には

、レシーバ201のSAM210のID、その登録リストの有効期限、バージョン番号、接続されている機器の数（この例では、レシーバ201には、レシーバ51の1機が接続され、自分自身を含めた合計数2）が記憶されている。リスト部には、図30のレシーバ51の登録リストのリスト部と同様の情報が記憶されている。

#### （6）コンテンツの購入及び利用

次に、EMDシステムの処理について、図33のフローチャートを参照して説明するが、ここでは、コンテンツプロバイダ2に保持されているコンテンツAが、サービスプロバイダ3を介して、ユーザホームネットワーク5のレシーバ51に供給され、利用される場合を例として説明する。

##### （6-1）EMDサービスセンタからコンテンツプロバイダへの配送用鍵の伝送

ステップS11において、配送用鍵Kdが、EMDサービスセンタ1からコンテンツプロバイダ2に供給される処理が行われる。この処理の詳細は、図34のフローチャートに示されている。すなわち、ステップS31において、EMDサービスセンタ1の相互認証部17（図3）は、コンテンツプロバイダ2の相互認証部39（図8）と相互認証し、コンテンツプロバイダ2が、正当なプロバイダであることが確認した後、EMDサービスセンタ1のコンテンツプロバイダ管理部12は、鍵サーバ14から供給された配送用鍵Kdをコンテンツプロバイダ2に送信する。なお、相互認証処理の詳細は、図35乃至図37を参照して後述する。

次に、ステップS32において、コンテンツプロバイダ2の暗号化部36は、EMDサービスセンタ1から送信された配送用鍵Kdを受信し、ステップS33において、記憶する。

このように、コンテンツプロバイダ2の暗号化部36が、配送用鍵Kdを記憶したとき、処理は終了し、図33のステップS12に進む。ここで、ステップS12の処理の説明の前に、図34のステップS31における相互認証処理（なり

すましがないことを確認する処理) について、1つの共通鍵を用いる場合(図35)、2つの共通鍵を用いる場合(図36)、および公開鍵暗号を用いる場合(図37)を例として説明する。

図35は、1つの共通鍵で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相互認証の動作を説明するフローチャートである。ステップS41において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数R1を生成する(乱数生成部35が生成するようにしてもよい)。ステップS42において、コンテンツプロバイダ2の相互認証部39は、DESを用いて乱数R1を、予め記憶している共通鍵Kcで暗号化する(暗号化部36で暗号化するようにしてもよい)。ステップS43において、コンテンツプロバイダ2の相互認証部39は、暗号化された乱数R1をEMDサービスセンタ1の相互認証部17に送信する。

ステップS44において、EMDサービスセンタ1の相互認証部17は、受信した乱数R1を予め記憶している共通鍵Kcで復号する。ステップS45において、EMDサービスセンタ1の相互認証部17は、32ビットの乱数R2を生成する。ステップS46において、EMDサービスセンタ1の相互認証部17は、復号した64ビットの乱数R1の下位32ビットを乱数R2で入れ替え、接続 $R_{1_H} \parallel R_2$ を生成する。なお、ここで $R_{i_H}$ は、 $R_i$ の上位nビットを表し、 $A \parallel B$ は、AとBの接続(nビットのAの下位に、mビットのBを結合して、(n+m)ビットとしたもの)を表す。ステップS47において、EMDサービスセンタ1の相互認証部17は、DESを用いて $R_{1_H} \parallel R_2$ を共通鍵Kcで暗号化する。ステップS48において、EMDサービスセンタ1の相互認証部17は、暗号化した $R_{1_H} \parallel R_2$ をコンテンツプロバイダ2に送信する。

ステップS49において、コンテンツプロバイダ2の相互認証部39は、受信した $R_{1_H} \parallel R_2$ を共通鍵Kcで復号する。ステップS50において、コンテンツプロバイダ2の相互認証部39は、復号した $R_{1_H} \parallel R_2$ の上位32ビット $R_{1_H}$ を調べ、ステップS41で生成した、乱数R1の上位32ビット $R_{1_H}$ と一

致すれば、EMDサービスセンタ1が正当なセンタであることを認証する。生成した乱数 $R_{1H}$ と、受信した $R_{1H}$ が一致しないとき、処理は終了される。両者が一致するとき、ステップS51において、コンテンツプロバイダ2の相互認証部39は、32ビットの乱数 $R_3$ を生成する。ステップS52において、コンテンツプロバイダ2の相互認証部39は、受信して復号した $R_{1H} \parallel R_2$ から下位32ビットを取り出した乱数 $R_2$ を上位に設定し、生成した乱数 $R_3$ をその下位に設定し、接続 $R_2 \parallel R_3$ とする。ステップS53において、コンテンツプロバイダ2の相互認証部39は、DESを用いて接続 $R_2 \parallel R_3$ を共通鍵 $K_c$ で暗号化する。ステップS54において、コンテンツプロバイダ2の相互認証部39は、暗号化された接続 $R_2 \parallel R_3$ をEMDサービスセンタ1の相互認証部17に送信する。

ステップS55において、EMDサービスセンタ1の相互認証部17は、受信した接続 $R_2 \parallel R_3$ を共通鍵 $K_c$ で復号する。ステップS56において、EMDサービスセンタ1の相互認証部17は、復号した接続 $R_2 \parallel R_3$ の上位32ビットを調べ、乱数 $R_2$ と一致すれば、コンテンツプロバイダ2を正当なプロバイダとして認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

図36は、2つの共通鍵 $K_{c1}$ ,  $K_{c2}$ で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相互認証の動作を説明するフローチャートである。ステップS61において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数 $R_1$ を生成する。ステップS62において、コンテンツプロバイダ2の相互認証部39は、DESを用いて乱数 $R_1$ を予め記憶している共通鍵 $K_{c1}$ で暗号化する。ステップS63において、コンテンツプロバイダ2の相互認証部39は、暗号化された乱数 $R_1$ をEMDサービスセンタ1に送信する。

ステップS64において、EMDサービスセンタ1の相互認証部17は、受信した乱数 $R_1$ を予め記憶している共通鍵 $K_{c1}$ で復号する。ステップS65において、EMDサービスセンタ1の相互認証部17は、乱数 $R_1$ を予め記憶してい

る共通鍵 $K_c 2$ で暗号化する。ステップS 6 6において、EMDサービスセンタ1の相互認証部1 7は、64ビットの乱数 $R_2$ を生成する。ステップS 6 7において、EMDサービスセンタ1の相互認証部1 7は、乱数 $R_2$ を共通鍵 $K_c 2$ で暗号化する。ステップS 6 8において、EMDサービスセンタ1の相互認証部1 7は、暗号化された乱数 $R_1$ および乱数 $R_2$ をコンテンツプロバイダ2の相互認証部3 9に送信する。

ステップS 6 9において、コンテンツプロバイダ2の相互認証部3 9は、受信した乱数 $R_1$ および乱数 $R_2$ を予め記憶している共通鍵 $K_c 2$ で復号する。ステップS 7 0において、コンテンツプロバイダ2の相互認証部3 9は、復号した乱数 $R_1$ を調べ、ステップS 6 1で生成した乱数 $R_1$ （暗号化する前の乱数 $R_1$ ）と一致すれば、EMDサービスセンタ1を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップS 7 1において、コンテンツプロバイダ2の相互認証部3 9は、復号して得た乱数 $R_2$ を共通鍵 $K_c 1$ で暗号化する。ステップS 7 2において、コンテンツプロバイダ2の相互認証部3 9は、暗号化された乱数 $R_2$ をEMDサービスセンタ1に送信する。

ステップS 7 3において、EMDサービスセンタ1の相互認証部1 7は、受信した乱数 $R_2$ を共通鍵 $K_c 1$ で復号する。ステップS 7 4において、EMDサービスセンタ1の相互認証部1 7は、復号した乱数 $R_2$ が、ステップS 6 6で生成した乱数 $R_2$ （暗号化する前の乱数 $R_2$ ）と一致すれば、コンテンツプロバイダ2を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

図3 7は、公開鍵暗号である、160ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ2の相互認証部3 9とEMDサービスセンタ1の相互認証部1 7との相互認証の動作を説明するフローチャートである。ステップS 8 1において、コンテンツプロバイダ2の相互認証部3 9は、64ビットの乱数 $R_1$ を生成する。ステップS 8 2において、コンテンツプロバイダ2の相互認証部3 9は、自分自身の公開鍵 $K_{p c p}$ を含む証明書（認証局から予め取得しておいたもの）

と、乱数 $R_1$ をEMDサービスセンタ1の相互認証部17に送信する。

ステップS83において、EMDサービスセンタ1の相互認証部17は、受信した証明書の署名（認証局の秘密鍵 $K_{sca}$ で暗号化されている）を、予め取得しておいた認証局の公開鍵 $K_{pca}$ で復号し、コンテンツプロバイダ2の公開鍵 $K_{pcp}$ とコンテンツプロバイダ2の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているコンテンツプロバイダ2の公開鍵 $K_{pcp}$ およびコンテンツプロバイダ2の名前を取り出す。証明書が認証局が発行した適正なものであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵 $K_{pcp}$ およびコンテンツプロバイダ2の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ2の公開鍵 $K_{pcp}$ およびコンテンツプロバイダ2の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵 $K_{pcp}$ が改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

適正な認証結果が得られたとき、ステップS84において、EMDサービスセンタ1の相互認証部17は、64ビットの乱数 $R_2$ を生成する。ステップS85において、EMDサービスセンタ1の相互認証部17は、乱数 $R_1$ および乱数 $R_2$ の接続 $R_1 \parallel R_2$ を生成する。ステップS86において、EMDサービスセンタ1の相互認証部17は、接続 $R_1 \parallel R_2$ を自分自身の秘密鍵 $K_{sesc}$ で暗号化する。ステップS87において、EMDサービスセンタ1の相互認証部17は、接続 $R_1 \parallel R_2$ を、ステップS83で取得したコンテンツプロバイダ2の公開鍵 $K_{pcp}$ で暗号化する。ステップS88において、EMDサービスセンタ1の相互認証部17は、秘密鍵 $K_{sesc}$ で暗号化された接続 $R_1 \parallel R_2$ 、公開鍵 $K_{pcp}$ で暗号化された接続 $R_1 \parallel R_2$ 、および自分自身の公開鍵 $K_{pesc}$ を含む証明書（認証局から予め取得しておいたもの）をコンテンツプロバイダ2の相互認証部39に送信する。

ステップS 8 9において、コンテンツプロバイダ2の相互認証部3 9は、受信した証明書の署名を予め取得しておいた認証局の公開鍵 $K_{pca}$ で復号し、正しければ証明書から公開鍵 $K_{pesc}$ を取り出す。この場合の処理は、ステップS 8 3における場合と同様であるので、その説明は省略する。ステップS 9 0において、コンテンツプロバイダ2の相互認証部3 9は、EMDサービスセンタ1の秘密鍵 $K_{sesc}$ で暗号化されている接続 $R_1 \parallel R_2$ を、ステップS 8 9で取得した公開鍵 $K_{pesc}$ で復号する。ステップS 9 1において、コンテンツプロバイダ2の相互認証部3 9は、自分自身の公開鍵 $K_{pcp}$ で暗号化されている接続 $R_1 \parallel R_2$ を、自分自身の秘密鍵 $K_{scp}$ で復号する。ステップS 9 2において、コンテンツプロバイダ2の相互認証部3 9は、ステップS 9 0で復号された接続 $R_1 \parallel R_2$ と、ステップS 9 1で復号された接続 $R_1 \parallel R_2$ を比較し、一致すればEMDサービスセンタ1を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

適正な認証結果が得られたとき、ステップS 9 3において、コンテンツプロバイダ2の相互認証部3 9は、64ビットの乱数 $R_3$ を生成する。ステップS 9 4において、コンテンツプロバイダ2の相互認証部3 9は、ステップS 9 0で取得した乱数 $R_2$ および生成した乱数 $R_3$ の接続 $R_2 \parallel R_3$ を生成する。ステップS 9 5において、コンテンツプロバイダ2の相互認証部3 9は、接続 $R_2 \parallel R_3$ を、ステップS 8 9で取得した公開鍵 $K_{pesc}$ で暗号化する。ステップS 9 6において、コンテンツプロバイダ2の相互認証部3 9は、暗号化した接続 $R_2 \parallel R_3$ をEMDサービスセンタ1の相互認証部1 7に送信する。

ステップS 9 7において、EMDサービスセンタ1の相互認証部1 7は、暗号化された接続 $R_2 \parallel R_3$ を自分自身の秘密鍵 $K_{sesc}$ で復号する。ステップS 9 8において、EMDサービスセンタ1の相互認証部1 7は、復号した乱数 $R_2$ が、ステップS 8 4で生成した乱数 $R_2$ （暗号化する前の乱数 $R_2$ ）と一致すれば、コンテンツプロバイダ2を適正なプロバイダとして認証し、一致しなければ、不適正なプロバイダとして、処理を終了する。

(6-2) コンテンツプロバイダからサービスプロバイダへのコンテンツの伝送

以上のように、EMDサービスセンタ1の相互認証部17とコンテンツプロバイダ2の相互認証部39は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵 $K_{temp}$ として利用される。

次に、図33のステップS12の処理について説明する。ステップS12においては、コンテンツプロバイダセキュアコンテナが、コンテンツプロバイダ2からサービスプロバイダ3に供給される処理が行われる。その処理の詳細は、図38のフローチャートに示されている。すなわち、ステップS201において、コンテンツプロバイダ2のウォータマーク付加部32(図8)は、コンテンツサーバ31からコンテンツAを読み出し、コンテンツプロバイダ2を示す所定のウォータマーク(電子透かし)を挿入し、圧縮部33に供給する。

ステップS202において、コンテンツプロバイダ2の圧縮部33は、ウォータマークが挿入されたコンテンツAをATRA C2等の所定の方式で圧縮し、暗号化部34に供給する。ステップS203において、乱数発生部35は、コンテンツ鍵 $K_{coA}$ となる乱数を発生させ、暗号化部34に供給する。

ステップS204において、コンテンツプロバイダ2の暗号化部34は、DESなどの所定の方式で、乱数発生部35で発生された乱数(コンテンツ鍵 $K_{coA}$ )を使用して、ウォータマークが挿入されて圧縮されたコンテンツAを暗号化する。次に、ステップS205において、暗号化部36は、DESなどの所定の方式で、EMDサービスセンタ1から供給された配送用鍵 $K_d$ でコンテンツ鍵 $K_{coA}$ を暗号化する。

ステップS206において、コンテンツプロバイダ2のセキュアコンテナ作成部38は、コンテンツA(コンテンツ鍵 $K_{coA}$ で暗号化されている)、コンテンツ鍵 $K_{coA}$ (配送用鍵 $K_d$ で暗号化されている)、およびポリシー記憶部37に記憶されている、コンテンツAに対応するUCPA, B(図9)の全体にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵 $K_{scp}$ で暗号化

する。これにより、図14に示した署名が作成される。

ステップS207において、コンテンツプロバイダ2のセキュアコンテナ作成部38は、コンテンツA（コンテンツ鍵K<sub>coA</sub>で暗号化されている）、コンテンツ鍵K<sub>coA</sub>（配送用鍵K<sub>d</sub>で暗号化されている）、UCPA、B（図9）、およびステップS206で生成した署名を含んだ、図14に示したコンテンツプロバイダセキュアコンテナを作成する。

ステップS208において、コンテンツプロバイダ2の相互認証部39は、サービスプロバイダ3の相互認証部45（図16）と相互認証する。この認証処理は、図35乃至図37を参照して説明した場合と同様であるので、その説明は省略する。ステップS209において、コンテンツプロバイダ2のセキュアコンテナ作成部38は、認証局から予め発行された証明書（図15）を、ステップS207で作成したコンテンツプロバイダセキュアコンテナに付して、サービスプロバイダ3に送信する。

このようにして、コンテンツプロバイダセキュアコンテナが、サービスプロバイダ3に供給されたとき、処理は終了し、図33のステップS13に進む。

#### （6-3）サービスプロバイダからレシーバへのコンテンツの伝送

ステップS13において、サービスプロバイダセキュアコンテナが、サービスプロバイダ3からユーザホームネットワーク5（レシーバ51）に供給される。この処理の詳細は、図39のフローチャートに示されている。すなわち、ステップS221において、サービスプロバイダ3の値付け部42（図16）は、コンテンツプロバイダ2から送信されたコンテンツプロバイダセキュアコンテナに付された証明書（図15）に含まれる署名を確認し、証明書の改竄がなければ、それから、コンテンツプロバイダ2の公開鍵K<sub>pcp</sub>を取り出す。証明書の署名の確認は、図37のステップS83における処理と同様であるので、その説明は省略する。

ステップS222において、サービスプロバイダ3の値付け部42は、コンテンツプロバイダ2から送信されたコンテンツプロバイダセキュアコンテナの署名

をコンテンツプロバイダ2の公開鍵 $K_{pcp}$ で復号し、得られたハッシュ値が、コンテンツA（コンテンツ鍵 $K_{coA}$ で暗号化されている）、コンテンツ鍵 $K_{coA}$ （配送用鍵 $K_d$ で暗号化されている）、およびUCPA, Bの全体にハッシュ関数を適用して得られたハッシュ値と一致するか否かを判定し、コンテンツプロバイダセキュアコンテナの改竄がないことを確認する。両者の値が一致しない場合（改竄が発見された場合）は、処理は終了されるが、この例の場合、コンテンツプロバイダセキュアコンテナの改竄はなかったものとし、ステップS223に進む。

ステップS223において、サービスプロバイダ3の値付け部42は、コンテンツプロバイダセキュアコンテナから、コンテンツA（コンテンツ鍵 $K_{coA}$ で暗号化されている）、コンテンツ鍵 $K_{coA}$ （配送用鍵 $K_d$ で暗号化されている）、および署名を取り出し、コンテンツサーバ41に供給する。コンテンツサーバ41は、それらを記憶する。値付け部42はまたUCPA, Bも、コンテンツプロバイダセキュアコンテナから取り出し、セキュアコンテナ作成部44に供給する。

ステップS224において、サービスプロバイダ3の値付け部42は、取り出したUCPA, Bに基づいて、PTA-1, A-2（図17）、およびPTB-1, B-2（図19）を作成し、セキュアコンテナ作成部44に供給する。

ステップS225において、サービスプロバイダ3のセキュアコンテナ作成部44は、コンテンツサーバ41から読み出したコンテンツA（コンテンツ鍵 $K_{coA}$ で暗号化されている）、コンテンツ鍵 $K_{coA}$ （配送用鍵 $K_d$ で暗号化されている）、およびコンテンツプロバイダ2の署名、値付け部42から供給された、UCPA, B、およびPTA-1, A-2, B-1, B-2、並びにその署名から、図21に示したサービスプロバイダセキュアコンテナを作成する。

ステップS226において、サービスプロバイダ3の相互認証部45は、レシーバ51の相互認証モジュール71（図23）と相互認証する。この認証処理は、図35乃至図37を参照して説明した場合と同様であるので、その説明を省略

する。

ステップS 2 2 7において、サービスプロバイダ3のセキュアコンテナ作成部4 4は、ステップS 2 2 5で作成したサービスプロバイダセキュアコンテナに、サービスプロバイダ3の証明書（図2 2）を付して、ユーザホームネットワーク5のレシーバ5 1に送信する。

このようにして、サービスプロバイダセキュアコンテナが、サービスプロバイダ3からレシーバ5 1に送信されたとき、処理は終了し、図3 3のステップS 1 4に進む。

#### （6－4）レシーバによるコンテンツの記録処理

ステップS 1 4において、サービスプロバイダ3から送信されたサービスプロバイダセキュアコンテナが、ユーザホームネットワーク5のレシーバ5 1により受信される。この処理の詳細は、図4 0のフローチャートに示されている。すなわち、ステップS 2 4 1において、レシーバ5 1の相互認証モジュール7 1（図2 3）は、通信部6 1を介して、サービスプロバイダ3の相互認証部4 5（図1 6）と相互認証し、相互認証できたとき、通信部6 1は、相互認証したサービスプロバイダ3－1から、サービスプロバイダセキュアコンテナ（図2 1）を受信する。相互認証できなかった場合、処理は終了されるが、この例の場合、相互認証されたものとし、ステップS 2 4 2に進む。

ステップS 2 4 2において、レシーバ5 1の通信部6 1は、ステップS 2 4 1で相互認証したサービスプロバイダ3から、公開鍵証明書を受信する。

ステップS 2 4 3において、レシーバ5 1の復号／暗号化モジュール7 4は、ステップS 2 4 1で受信したサービスプロバイダセキュアコンテナに含まれる署名を検証し、改竄がなかったか否かを検証する。ここで、改竄が発見された場合、処理は終了するが、この例の場合、改竄が発見されなかったものとし、ステップS 2 4 4に進む。

ステップS 2 4 4において、レシーバ5 1の記憶モジュール7 3に記憶されている基準情報5 1（図2 9）に基づいて、利用条件を満たすUCPと価格条件を

満たすP Tが選択され、表示制御部67を介して、図示せず表示部に表示される。ユーザは、表示されたUCPおよびP Tの内容を参照して、図示せぬ操作部を操作し、UCPの1つの利用内容を選択する。これにより、入力制御部68は、操作部から入力された、ユーザの操作に対応する信号をSAM62に出力する。

この例の場合、レシーバ51の基準情報51の「利用ポイント情報」には、利用ポイントが222ポイントであるとされているものとする。すなわち、コンテンツAに対応して設定されたUCPA、Bのうち、「利用条件10」の「ユーザ条件10」が“200ポイント以上”とされている、UCPAが選択される。また、基準情報51の「決済ユーザ情報」には、ユーザは男性とされているので、PTA-1（図17A）の「価格条件10」に設定された条件を満たす。その結果、UCPAに対応して作成されたPTA-1、PTA-2のうち、PTA-1が選択される。結局、UCPAおよびPTA-1の内容が、表示部に表示される。また、この例の場合、これにより、ユーザが、UCPAの利用内容11（PTA-1の価格内容11）を選択したものとする。

ステップS245において、レシーバ51のSAM62の課金処理モジュール72は、ステップS244で選択された、UCPAの「利用内容11」の内容（PTA-1の「価格内容11」の内容）に基づいて、UCSA（図25）および課金情報A（図27）を作成する。すなわち、この場合、コンテンツAは、料金が2000円で買い取り再生される。

ステップS246において、サービスプロバイダセキュアコンテナ（図21）に含まれる、コンテンツA（コンテンツ鍵KcoAで暗号化されている）、UCPA、PTA-1、A-2、およびコンテンツプロバイダ2の署名が取り出され、HDD52に出力され、記憶される。ステップS247において、復号／暗号化ユニット74の復号ユニット91は、サービスプロバイダセキュアコンテナに含まれるコンテンツ鍵KcoA（配送用鍵Kdで暗号化されている）を、記憶モジュール73に記憶されている配送用鍵Kdで復号する。

ステップS248において、復号／暗号化ユニット74の暗号化ユニット93

は、ステップS 2 4 7で復号されたコンテンツ鍵K c o Aを、記憶モジュール7 3に記憶されている保存用鍵K s a v eで暗号化する。

ステップS 2 4 9において、S A M 6 2のデータ検査モジュール7 5は、ステップS 2 4 8で保存用鍵K s a v eで暗号化されたコンテンツ鍵K c o A、およびステップS 2 4 5で作成されたU C S Aが対応して記憶される、外部記憶部6 3の利用情報記憶部6 3 A（図2 6）の空き領域を有するブロックB Pを検出する。この例の場合、利用情報記憶部6 3 AのブロックB P - 1が検出される。なお、図2 6の利用情報記憶部6 3 Aにおいて、そのブロックB P - 1の利用情報用メモリ領域R P - 3にコンテンツ鍵K c o AおよびU C S Aが記憶されているように示されているが、この例の場合、この時点において、それらは記憶されておらず、ブロックB P - 1の利用情報用メモリ領域R P - 3は、空いており、所定の初期情報が記憶されているものとする。

ステップS 2 5 0において、レシーバ5 1のデータ検査モジュール7 5は、ステップS 2 4 9で検出したブロックB P - 1のデータ（利用情報用メモリ領域R P - 1乃至R P - Nに記憶されている全てのデータ）にハッシュ関数を適用して、ハッシュ値を得る。次に、ステップS 2 5 1において、データ検査モジュール7 5は、ステップS 2 5 0で得られたハッシュ値と、記憶モジュール7 3に記憶されているブロックB P - 1に対応する検査値H P - 1（図2 8）とを比較し、一致するか否かを判定し、一致すると判定した場合、そのブロックB P - 1のデータは改竄されていないので、ステップS 2 5 2に進む。

ステップS 2 5 2において、レシーバ5 1のS A M 6 2は、利用情報（ステップS 2 4 8で、保存用鍵K s a v eで暗号化されたコンテンツ鍵K c o A、およびステップS 2 4 5で作成されたU C S A（図2 5））を、図2 6に示すように、利用情報記憶部6 3 A（外部記憶部6 3）のブロックB P - 1の利用情報用メモリ領域R P - 3に記憶させる。

ステップS 2 5 3において、レシーバ5 1のデータ検査モジュール7 5は、ステップS 2 5 2で利用情報が記憶された利用情報用メモリ領域R P - 3が属する

、利用情報記憶部 6 3 A のブロック B P - 1 のデータにハッシュ関数を適用し、ハッシュ値を算出し、ステップ S 2 5 4 において、記憶モジュール 7 3 に記憶されている検査値 H P - 1 に上書きする。ステップ S 2 5 5 において、課金処理モジュール 7 2 は、ステップ S 2 4 5 で作成した課金情報 A を記憶モジュール 7 3 に記憶させ、処理は終了する。

ステップ S 2 5 1 において、算出されたハッシュ値と検査値 H P - 1 とが一致しないと判定された場合、ブロック B P - 1 のデータは改竄されているので、手続きは、ステップ S 2 5 6 に進み、データ検査モジュール 7 5 は、外部記憶部 6 3 の利用情報記憶部 6 3 A の全てのブロック B P を調べたか否かを判定し、外部記憶部 6 3 の全てのブロック B P を調べていないと判定した場合、ステップ S 2 5 7 に進み、利用情報記憶部 6 3 A の、調べていない（空きを有する他の）ブロック B P を検索し、ステップ S 2 5 0 に戻り、それ以降の処理が実行される。

ステップ S 2 5 6 において、外部記憶部 6 3 の利用情報記憶部 6 3 A の全てのブロック B P が調べられたと判定された場合、利用情報を記憶できるブロック B P（利用情報用メモリ領域 R P）は存在しないので、処理は終了する。

このように、サービスプロバイダセキュアコンテナが、レシーバ 5 1 により受信されると、処理は終了し、図 3 3 のステップ S 1 5 に進む。

#### （ 6 - 4 ）コンテンツの再生処理

ステップ S 1 5 において、供給されたコンテンツ A が、レシーバ 5 1 において利用される。なお、この例の場合、図 4 0 のステップ S 2 2 4 で選択された U C P A の利用内容 1 1 によれば、コンテンツ A は、再生して利用される。そこで、ここでは、コンテンツ A の再生処理について説明する。この再生処理の詳細は、図 4 1 のフローチャートに示されている。

ステップ S 2 6 1 において、レシーバ 5 1 のデータ検査モジュール 7 5 は、図 4 0 のステップ S 2 5 2 で、コンテンツ鍵 K c o A（保存用鍵 K s a v e で暗号化されている）および U C S A が記憶された利用情報用メモリ領域 R P - 3 が属する、外部記憶部 6 3 の利用情報記憶部 6 3 A のブロック B P - 1 のデータにハ

ッシュ関数を適用してハッシュ値を算出する。

ステップS 2 6 2において、レシーバ5 1のデータ検査モジュール7 5は、ステップS 2 6 1において算出したハッシュ値が、図4 0のステップS 2 5 3で算出し、ステップS 2 5 4で記憶モジュール7 3に記憶させたハッシュ値（検査値HP-1）と一致するか否かを判定し、一致すると判定した場合、ブロックBP-1のデータは改竄されていないので、ステップS 2 6 3に進む。

ステップS 2 6 3において、UCSA（図2 5）の「利用内容」の「パラメータ」に示されている情報に基づいて、コンテンツAが利用可能か否かが判定される。例えば、「利用内容」の「形式」が、「期間制限再生」とされているUCSにおいては、その「パラメータ」には、その開始期間（時刻）と終了期間（時刻）が記憶されているので、この場合、現在の時刻が、その範囲内にあるか否かが判定される。すなわち、現在時刻が、その範囲内にあるとき、そのコンテンツの利用が可能であると判定され、範囲外にあるとき、利用不可と判定される。また、「利用内容」の「形式」が、所定の回数に限って再生（複製）する利用形式とされているUCSにおいては、その「パラメータ」には、残された利用可能回数が記憶されている。この場合、「パラメータ」に記憶されている利用可能回数が0回でないとき、対応するコンテンツの利用が可能であると判定され、一方、利用可能回数が0回であるとき、利用不可と判定される。

なお、UCSAの「利用内容」の「形式」は、「買い取り再生」とされているので、この場合、コンテンツAは、買い取られ、制限なしに再生される。すなわち、UCSAの「利用内容」の「パラメータ」には、コンテンツが利用可能であることを示す情報が設定されている。そのため、この例の場合では、ステップS 2 6 3において、コンテンツAが利用可能であると判定され、ステップS 2 6 4に進む。

ステップS 2 6 4において、レシーバ5 1の課金モジュール7 2は、UCSAを更新する。UCSAには、更新すべき情報は含まれていないが、例えば、「利用内容」の「形式」が所定の回数に限って再生する利用形式とされている場合、

その「パラメータ」に記憶されている、再生可能回数が1つだけデクリメントされる。

次に、ステップS 2 6 5において、レシーバ5 1のSAM 6 2は、ステップS 2 6 4で更新されたUCSA（この例の場合には、実際は、更新されていない）を、外部記憶部6 3の利用情報記憶部6 3 AのブロックBP-1の利用情報用メモリ領域RP-3に記憶させる。ステップS 2 6 6において、データ検査モジュール7 5は、ステップS 2 6 5でUCSAが記憶された、外部記憶部6 3の利用情報記憶部6 3 AのブロックBP-1のデータにハッシュ関数を適用して、ハッシュ値を算出し、記憶モジュール7 3に記憶されている検査値HP-1に上書きする。

ステップS 2 6 7において、SAM 6 2の相互認証モジュール7 1と、伸張部6 4の相互認証モジュール1 0 1は、相互認証し、SAM 6 2および伸張部6 4は、一時鍵K t e m pを共有する。この認証処理は、図3 5乃至図3 7を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数R 1、R 2、R 3、またはその組み合わせが、一時鍵K t e m pとして用いられる。

ステップS 2 6 8において、復号／暗号化モジュール7 4の復号ユニット9 1は、図4 0のステップS 2 5 2で外部記憶部6 3の利用情報記憶部6 3 AのブロックBP-1（利用情報用メモリ領域RP-3）に記憶されたコンテンツ鍵K c o A（保存用鍵K s a v eで暗号化されている）を、記憶モジュール7 3に記憶された保存用鍵K s a v eで復号する。

次に、ステップS 2 6 9において、復号／暗号化モジュール7 4の暗号化ユニット9 3は、復号されたコンテンツ鍵K c o Aを一時鍵K t e m pで暗号化する。ステップS 2 7 0において、SAM 6 2は、一時鍵K t e m pで暗号化されたコンテンツ鍵K c o Aを伸張部6 4に送信する。

ステップS 2 7 1において、伸張部6 4の復号モジュール1 0 2は、コンテンツ鍵K c o Aを一時鍵K t e m pで復号する。ステップS 2 7 2において、伸張

部 6 4 は、インタフェース 6 6 を介して、HDD 5 2 に記録されたコンテンツ A（コンテンツ鍵 K c o で暗号化されている）を受け取る。ステップ S 2 7 3 において、伸張部 6 4 の復号モジュール 1 0 3 は、コンテンツ A（コンテンツ鍵 K c o で暗号化されている）をコンテンツ鍵 K c o A で復号する。

ステップ S 2 7 4 において、伸張部 6 4 の伸張モジュール 1 0 4 は、復号されたコンテンツ A を A T R A C 2 などの所定の方式で伸張する。ステップ S 2 7 5 において、伸張部 6 4 のウォーターマーク付加モジュール 1 0 5 は、伸張されたコンテンツ A にレシーバ 5 1 を特定する所定のウォーターマーク（電子透かし）を挿入する。ステップ S 2 7 6 において、コンテンツ A は、図示せぬスピーカなどに出力され、処理は終了する。

ステップ S 2 6 2 において、ステップ S 2 6 1 において算出されたハッシュ値が、レシーバ 5 1 の記憶モジュール 7 3 に記憶されたハッシュ値と一致しないと判定された場合、またはステップ S 2 6 3 において、コンテンツが利用不可と判定された場合、ステップ S 2 7 7 において、S A M 6 2 は、表示制御部 6 7 を介して、図示せぬ表示部にエラーメッセージを表示させる等の所定のエラー処理を実行し、処理は終了する。

このようにして、レシーバ 5 1 において、コンテンツ A が再生（利用）されたとき、処理は終了し、図 3 3 の処理も終了する。

#### （6－5）決済処理

次に、レシーバ 5 1 において計上された課金を決済する場合の処理手順を、図 4 2 のフローチャートを参照して説明する。なお、この処理は、計上された課金が所定の上限額（正式登録時の上限額または仮登録時の上限額）を越えた場合、または配送用鍵 K d のバージョンが古くなり、例えば、図 4 0 のステップ S 2 4 7 で、コンテンツ鍵 K c o（配送用鍵 K d で暗号化されている）を復号することができなくなった場合（サービスプロバイダセキュアコンテナを受信することができなくなった場合）に開始される。

ステップ S 3 0 1 において、レシーバ 5 1 と EMD サービスセンタ 1 との相互

認証が行われる。この相互認証は、図35乃至図37を参照して説明した場合と同様の処理であるので、その説明は省略する。

次に、ステップS302において、レシーバ51のSAM62は、EMDサービスセンタ1のユーザ管理部18（図3）に証明書を送信する。ステップS303において、レシーバ51のSAM62は、記憶モジュール73に記憶されている課金情報を、ステップS301でEMDサービスセンタ1と共有した一時鍵Ktempで暗号化し、配送用鍵Kdのバージョン、対応するUCPとPT、並びに登録リストとともに、EMDサービスセンタ1に送信する。

ステップS304において、EMDサービスセンタ1のユーザ管理部18は、ステップS303で、レシーバ51から送信された情報を受信し、復号した後、EMDサービスセンタ1のユーザ管理部18が、登録リストの「状態フラグ」に“停止”が設定されるべき不正行為がレシーバ51において存在するか否かを確認する。

ステップS305において、EMDサービスセンタ1の課金請求部19は、ステップS303で受信された課金情報を解析し、ユーザ（例えば、ユーザF）の支払い金額を算出する処理等を行う。次に、ステップS306において、ユーザ管理部18は、ステップS305における処理により、決済が成功したか否かを確認する。

次に、ステップS307において、EMDサービスセンタ1のユーザ管理部18は、ステップS304における確認結果、およびステップS306における確認結果に基づいて、レシーバ51の登録条件を設定し、それに署名を付して、レシーバ51の登録リストを作成する。

例えば、ステップS304で、不正行為が確認された場合、「状態フラグ」には“停止”が設定され、この場合、今後、全ての処理が停止される。すなわち、EMDシステムからのサービスを一切受けることができなくなる。また、ステップS306で、決済が成功しなかったことが確認された場合、「状態フラグ」には“制限あり”が設定され、この場合、すでに購入したコンテンツを再生する処

理は可能とされるが、新たにコンテンツを購入する処理は実行できなくなる。

次に、ステップS 3 0 8に進み、EMDサービスセンタ1のユーザ管理部1 8は、最新バージョンの配送用鍵K d（3ヶ月分の最新バージョンの配送用鍵K d）およびステップS 3 0 7で作成された登録リストを、一時鍵K t e m pで暗号化し、レシーバ5 1に送信する。

ステップS 3 0 9において、レシーバ5 1のSAM 6 2は、EMDサービスセンタ1から送信された配送用鍵K dおよび登録リストを、通信部6 1を介して受信し、復号した後、記憶モジュール7 3に記憶させる。このとき、記憶モジュール7 3に記憶されていた課金情報は消去され、登録リストおよび配送用鍵K dが更新される。また、このとき、受信された登録リストの登録リスト署名が検証され、登録リストが改竄されていないとが確認される。この署名の確認処理は、図3 7のステップS 8 3における処理と同様であるので、その説明は省略する。

#### （6－6）代理決済処理

次に、レシーバ5 1が、レシーバ2 0 1において計上された課金を決済する場合（代理決済する場合）の処理手順を、図4 3乃至図4 5のフローチャートを参照して説明する。レシーバ5 1が、レシーバ2 0 1から、代理決済を依頼する所定の信号を受信すると、ステップS 3 2 1において、レシーバ5 1の相互認証モジュール7 1は、レシーバ2 0 1の相互認証モジュール2 2 1と相互認証を行う。この相互認証は、図3 7を参照して説明した場合と同様であるので、その説明は省略するが、これにより、レシーバ5 1の相互認証モジュール7 1は、レシーバ2 0 1のSAM 2 1 2のIDを取得し、レシーバ2 0 1と一時鍵K t e m pを共有する。

ステップS 3 2 2において、レシーバ5 1のSAM 6 2は、HDD 5 2に記憶されている登録リストが改竄されているか否かを判定する。具体的には、登録リストの「登録リスト署名」に記憶されている署名が、公開鍵暗号の公開鍵で復号され、その結果（ハッシュ値）と、その登録リストのデータの全体のハッシュ値とが、等しいか否かが判定される。

ステップS 3 2 2で、登録リストが改竄されていないと判定された場合、ステップS 3 2 3に進み、レシーバ5 1のSAM 6 2は、レシーバ2 0 1が、代理決済することができる（代理決済すべき）機器であるか否かを判定する。具体的には、ステップS 3 2 1で取得されたSAM 2 1 2のIDが、登録リストの「SAM ID」に登録され、そしてそれに対応する「課金機器」に自分自身（SAM 6 2）が登録されているか否かが判定される。

ステップS 3 2 3において、この例の場合のように、レシーバ2 0 1が代理決済することができる機器であると判定した場合、レシーバ5 1のSAM 6 2は、ステップS 3 2 4に進み、課金情報の提供を要求する所定の信号を通信部6 5を介して、レシーバ2 0 1に送信し、ステップS 3 2 5において、レシーバ2 0 1から送信されてきた課金情報を受信する。

ステップS 3 2 6において、レシーバ5 1は、EMDサービスセンタ1と相互認証する。この相互認証は、図3 5乃至図3 7を参照して説明した場合と同様であるので、その説明は省略する。ステップS 3 2 7において、レシーバ5 1のSAM 6 2は、ステップS 3 2 5で受信した課金情報、記憶モジュール7 3に記憶されている配送用鍵K dのバージョン、またHDD 5 2に記憶されている登録リストを、一時鍵K t e m pで暗号化し、EMDサービスセンタ1に送信する。

ステップS 3 2 8において、EMDサービスセンタ1のユーザ管理部1 8は、レシーバ5 1から送信された情報を受信し、復号した後、EMDサービスセンタ1の監査部2 1が、登録リストの「状態フラグ」に” 停止” が設定されるべき不正行為が、レシーバ5 1において存在するか否かを確認する。

次に、ステップS 3 2 9において、EMDサービスセンタ1のユーザ管理部1 8は、ステップS 3 2 8での確認結果に基づいて、レシーバ5 1に不正行為が存在するか否かを判定し、レシーバ5 1に不正行為が存在しないと判定した場合、ステップS 3 3 0に進む。

ステップS 3 3 0において、EMDサービスセンタ1の課金請求部1 9は、ステップS 3 2 8で受信された課金情報を解析し、ユーザの支払い金額を算出する

処理等を行う。次に、ステップS 3 3 1において、EMDサービスセンタ1のユーザ管理部18は、ステップS 3 3 0における決済の結果に基づいて、レシーバ51およびレシーバ201の登録条件を設定し、登録条件署名および登録リスト署名を付して、それぞれの登録リストを作成する。

次に、ステップS 3 3 2に進み、EMDサービスセンタ1のユーザ管理部18は、最新バージョンの配送用鍵K d、並びにステップS 3 3 1で作成されたレシーバ51の登録リストとレシーバ201の登録リストを、一時鍵K t e m pで暗号化して、レシーバ51に送信する。

ステップS 3 3 3において、レシーバ51のSAM62は、EMDサービスセンタ1から送信された配送用鍵K d、並びにレシーバ51の登録リストとレシーバ201の登録リストを受信し、復号すると、ステップS 3 3 4において、レシーバ51の登録リストの、レシーバ201のSAM212のIDに対応する「状態フラグ」に、動作制限情報（例えば、“制限あり”または“停止”が）設定されているか否かを判定し、それが設定されていない場合、ステップS 3 3 5に進む。

ステップS 3 3 5において、レシーバ51のSAM62は、ステップS 3 2 5で受信された、レシーバ201からの課金情報を消去し、ステップS 3 3 6において、配送用鍵K dおよびレシーバ51の登録リストを更新する。

次に、ステップS 3 3 7において、レシーバ51のSAM62は、レシーバ201に対して、相互認証（図33乃至図35を参照して説明した処理）を行った後、レシーバ201に、レシーバ201の登録リストと配送用鍵K dを一時鍵K t e m pで暗号化して、送信する。

ステップS 3 3 8において、レシーバ201は、レシーバ51から送信されてきたレシーバ201の登録リストおよび配送用鍵K dを受信し、一時鍵K t e m pで復号した後、記憶する（更新）する。

ステップS 3 3 4で、「状態フラグ」に動作制限情報が設定されていると判定された場合、ステップS 3 3 9に進み、レシーバ51のSAM62は、レシーバ

２０１に対して、所定の処理（ＲＥＶＯＫＥ処理）を実行し、レシーバ２０１において実行される処理を制限する。

ステップＳ３２９において、レシーバ５１において不正行為が確認された場合、ステップＳ３４０に進み、ＥＭＤサービスセンタ１は、レシーバ５１およびレシーバ２０１に対応する「状態フラグ」の全てに”停止”を設定し、それぞれの登録リストを作成し、ステップＳ３４１において、それらをレシーバ５１に送信する。

ステップＳ３４２において、レシーバ５１は、ＥＭＤサービスセンタ１から送信された登録リストを受信し、登録リストを更新する。その後、ステップＳ３３９に進み、レシーバ５１は、登録リストの「状態フラグ」に設定された動作制限情報に対応する処理を行う。この場合、配送用鍵Ｋｄは、レシーバ５１およびレシーバ２０１には供給されず、レシーバ５１およびレシーバ２０１は、供給されたコンテンツを再生することができなくなり、その結果、ＥＭＤシステムにおけるサービスを一切受けることができなくなる。

ステップＳ３２２において、登録リストが改竄されていると判定された場合、またステップＳ３２３において、代理決済することができる機器ではないと判定された場合、処理は終了される。

以上のようにして、レシーバ２０１において計上された課金が、レシーバ５１により代理決済させる。

#### （７）ユーザホームネットワークの他の構成例

図４６は、ユーザホームネットワーク５の他の構成例を表している。なお、図中、図１のユーザホームネットワーク５における場合と対応する部分については、同一の符号を付してある。すなわち、レシーバ２０１に代わり、Ｌ個のレシーバ２５１－１乃至２５１－Ｌ（以下、個々に区別する必要がない場合、単に、レシーバ２５１と称する。他の装置についても同様である）、およびＨＤＤ２０２に代わり、Ｌ個のＨＤＤ２５２－１乃至２５２－Ｌが設けられている。

レシーバ２５１－１乃至２５１－Ｌは、レシーバ２０１と同様の構成を有する

据え置き型の装置で、それぞれHDD252-1乃至252-Lに接続されている。レシーバ251はまた、レシーバ201と同様に、コンテンツを購入するための処理を実行することができるが、自分自身で課金を決済することができず、レシーバ51により代理決済されるようになされている。すなわち、例えば、この場合におけるレシーバ51の登録リスト（図47）およびレシーバ251-1の登録リスト（図48）に示すように、レシーバ251-i（=1, 2, ..., L）のSAMのIDに対応する「購入処理」には、“可”が設定され、「課金処理」には、“不可”が設定され、そして「課金機器」には“SAM62のID”が、それぞれ設定されている。

次に、レシーバ51が、レシーバ251において計上される課金を精算する場合の処理手順を、図49乃至図51のフローチャートを参照して説明する。

ステップS361において、レシーバ51のSAM62は、カウンタiに初期値1を設定し、ステップS362において、レシーバ51の相互認証モジュール71は、レシーバ251-i（=1, 2, ..., L）の相互認証モジュール（図示せず）と相互認証する。この相互認証は、図35乃至図37を参照して説明した場合と同様であるので、その説明は省略する。

ステップS363乃至S383においては、図43のステップS322乃至S342における場合と同様の処理が実行されるので、その説明は省略する。

ステップS379において、レシーバ251-iが配送鍵Kdおよび登録リストを更新した後、またはレシーバ51が、「状態フラグ」に設定された動作制限情報に対応した処理を行った後、ステップS384に進み、レシーバ51のSAM62は、カウンタiの値が、代理決済すべき機器の数（この例の場合、レシーバ251の数L）と等しいか否かを判定し、等しくないと判定した場合、ステップS385に進み、カウンタiの値を1だけ増加させて、ステップS362に戻る。これにより、次のレシーバ251-iに対応して、それ以降の処理が実行される。

ステップS384において、カウンタiの値と、代理決済すべき機器の数Lと

が等しいと判定された場合、処理は終了される。

ステップS 3 6 3において、登録リストが改竄されていると判定された場合、またステップS 3 6 4において、代理決済することができる機器ではないと判定された場合、処理は、ステップS 3 8 4に進む。

以上のようにして、L個のレシーバ2 5 1-1乃至2 5 1-Lにおいて、それぞれ計上される課金が、レシーバ5 1により代理決済される。なお、以上においては、レシーバ5 1が、一度に、レシーバ2 5 1の全てに対して、代理決済を行う場合を例として説明したが、図4 3乃至図4 5のフローチャートで説明したように、依頼があった機器に対してのみ代理決済を行うようにすることもできる。

なお、以上において、図4 3のステップS 3 2 3および図4 9のステップS 3 6 3における、登録リストが改竄されているか否かの判定は、「登録リスト署名」に記憶されている署名を確認することで行われたが、入力されたデータを、6 4ビットずつのブロックに切り分け、それを順次、処理時間の早いブロック暗号器に入力し、所定の検査用鍵で暗号化してそれを第1の出力とし、その第1び出力を遅延された第2の出力との排他的論理和により、データの改竄を確認するC B (Cipher Block Chaining) モードを利用することもできる。

図5 2は、ユーザホームネットワーク5の他の構成例を表している。なお、図中、図1のユーザホームネットワーク5における場合と対応する部分については、同一の符号を付してある。すなわち、レシーバ2 0 1およびHDD 2 0 2に代わり、レシーバ3 0 1、レシーバ4 0 1、およびHDD 4 0 2が設けられている。

図5 3は、レシーバ3 0 1の機能的構成例を表している。レシーバ3 0 1は、レシーバ2 0 1のSAM 2 1 2乃至通信部2 1 5と基本的に同様の機能を有する、SAM 3 1 1乃至通信部3 1 4を有しているが、レシーバ2 0 1の、通信部2 1 1、インタフェース2 1 6、表示制御部2 1 7、および入力制御部2 1 8に対応する機能を有しない、携帯型の機器である。

レシーバ301は、HDDに接続されていないので、コンテンツは、図54に示すような形態を有する、外部記憶部312の利用情報記憶部312Aに、コンテンツ鍵Kco（保存鍵Ksaveで暗号化されている）およびUCSと対応して記憶される。

図55に示すようなレシーバ301の登録リストは、記憶モジュール323に記憶されている。この登録リストの対象SAM情報部には、この登録リストを保有するレシーバ301のSAM311のIDが（「対象SAMID」の欄に）記憶され、その登録リストの有効期限が（「有効期限」の欄に）記憶され、登録リストのバージョン番号が（「バージョン番号」の欄に）記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ301には、レシーバ51の1機の機器が接続されているので、自分自身を含む合計値2が（「接続されている機器数」の欄に）記憶されている。リスト部には、図30のレシーバ51の登録リストの、レシーバ301の登録条件が記憶されているが、この場合、「登録条件署名」および「登録リスト署名」は、削除されている。これは、登録リストの署名の確認後、取り除かれたためで、これにより、記憶モジュール323の記憶容量を節約することができる。なお、この例の場合、1つの署名あたり、40バイトが必要とされる。

レシーバ301は、サービスプロバイダ2およびEMDサービスセンタ1と通信を行うことができないので、コンテンツを購入する処理を行うことができない。そのため、「購入処理」には、“不可”が記憶されている。このように、レシーバ301においては、コンテンツの購入がなされないので、課金は計上されない。そのため「課金処理」には“不可”が、そして「課金機器」には、“なし”が記憶される。

レシーバ301は、この例の場合、接続されるレシーバ51から、コンテンツの供給を受けるようになされているので、「コンテンツ供給機器」には、レシーバ51のSAM62のIDが記憶されている。

「状態フラグ」には、この例の場合“なし”が設定されている。「登録条件署

名」および「登録リスト署名」には、所定の署名が記憶されている。

図56は、レシーバ401の機能的構成例を表している。レシーバ401は、レシーバ201のSAM212乃至入力制御部218と基本的に同様の機能を有する、SAM311乃至入力制御部417を有しているが、レシーバ201の通信部211に対応する機能を有しない、据え置き型の機器である。

HDD402には、コンテンツ等の他、図57に示すような、レシーバ401の登録リストが記憶されている。この登録リストの対象SAM情報部には、この登録リストを保有するレシーバ401のSAM411のIDが（「対象SAMID」の欄に）記憶され、その登録リストの有効期限が記憶され、登録リストのバージョン番号が記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ401には、レシーバ51の1機の機器が接続されているので、自分自身を含む合計値2が（「接続されている機器数」の欄に）記憶されている。

リスト部の「SAMID」には、レシーバ401のSAM411のIDが記憶され、「ユーザID」には、レシーバ401のユーザのIDが記憶される。レシーバ401は、サービスプロバイダ2およびEMDサービスセンタ1と通信を行うことができないので、コンテンツを購入する処理を行うことができない。そのため、「購入処理」には、“不可”が記憶されている。

レシーバ401においては、コンテンツの購入がなされないので、課金は計上されない。そのため「課金処理」には“不可”が、「課金機器」には、“なし”が記憶される。レシーバ401は、接続されるレシーバ51からコンテンツの供給を受けるようになされているので、「コンテンツ供給機器」には、レシーバ51のSAM62のIDが記憶されている。

「状態フラグ」には、この例の場合“なし”が設定されている。「登録条件署名」および「登録リスト署名」には、所定の署名が記憶されている。

なお、この例の場合、レシーバ51の登録リストは、図58に示すように、レシーバ51の登録リストの他、図55の登録リストに示されるレシーバ301の

登録条件、および図 5 7 の登録リストに示されるレシーバ 4 0 1 の登録条件が設定されている。

次に、レシーバ 5 1 が、レシーバ 3 0 1 に代わり、コンテンツの購入処理を実行する場合の処理手順を、図 5 9 のフローチャートを参照して説明する。ステップ S 4 0 1 において、レシーバ 5 1 は、レシーバ 3 0 1 と相互認証を行う。この相互認証は、図 3 7 を参照して説明した場合と同様であるので、その説明は省略するが、これにより、レシーバ 5 1 の相互認証モジュール 7 1 は、レシーバ 3 0 1 の SAM 3 1 1 の ID を取得し、レシーバ 3 0 1 と一時鍵 K t e m p を共有する。

ステップ S 4 0 2 において、レシーバ 5 1 の SAM 6 2 は、HDD 5 2 に記憶されている登録リストが改竄されているか否かを判定する。具体的には、登録リストの「登録リスト署名」に記憶されている署名が、公開鍵暗号の公開鍵で復号され、それ結果（ハッシュ値）と、その登録リストのデータの全体のハッシュ値とが、等しいか否かが判定される。

ステップ S 4 0 2 で、登録リストが改竄されていないと判定された場合、ステップ S 4 0 3 に進み、レシーバ 5 1 の SAM 6 2 は、代理購入の依頼があったレシーバ 3 0 1 が、代理購入することができる機器であるか否かを判定する。具体的には、ステップ S 4 0 1 で取得された SAM 3 1 1 の ID が、登録リストの「SAM ID」に登録され、そしてそれに対応する「コンテンツ供給機器」に SAM 6 2 が登録されているか否かが判定される。この例の場合、レシーバ 5 1 の登録リスト（図 5 8）の「SAM ID」には、レシーバ 3 0 1 の SAM 3 1 1 の ID が設定され、そしてそれに対応する「コンテンツ供給機器」には、SAM 6 2 の ID が設定されているので、ステップ S 4 0 3 において、レシーバ 3 0 1 が、代理購入することができる機器であると判定され、ステップ S 4 0 4 に進む。

ステップ S 4 0 4 において、レシーバ 5 1 の SAM 6 2 は、代理購入が可能であることを示す所定の信号を、通信部 6 5 を介してレシーバ 3 0 1 に送信する。

レシーバ 3 0 1 の SAM 3 1 1 は、レシーバ 5 1 から、代理購入が可能である

ことを示す信号を受信すると、ステップS 4 0 5において、レシーバ3 0 1のデータ検査モジュール3 2 5は、購入するコンテンツAを記憶する、外部記憶部3 1 2の利用情報記憶部3 1 2 AのブロックB Pを検出する。

次に、ステップS 4 0 6において、レシーバ3 0 1のデータ検査モジュール3 2 5は、ステップS 4 0 5で検出した、利用情報記憶部3 1 2 AのブロックB Pのデータの全体にハッシュ関数を適用してハッシュ値を算出し、記憶モジュール3 2 3に記憶されている、検出されたブロックB Pに対応する検査値H Pと一致しているか否かを判定する。それらの値が一致すると判定された場合、すなわち、利用情報記憶部3 1 2 Aの、ステップS 4 0 5で検出されたブロックB Pのデータが改竄されていない場合、ステップS 4 0 7に進み、SAM 3 1 1は、コンテンツの供給を受け取ることが可能であることを示す所定の信号を、通信部3 1 4を介して、レシーバ5 1に送信する。

ステップS 4 0 8において、レシーバ5 1のSAM 6 2（課金モジュール7 2）は、選択されたUCPの「利用内容」とPTに基づいて、UCSおよび課金情報を作成する。具体的には、レシーバ5 1の表示制御部6 7が、UCPA, B（図9）、およびPTA-1, A-2（図17）、B-1, B-2（図19）の内容を、図示せぬ表示部に出力し、ユーザに提示する。ユーザは、提示されたこれらの情報から、この例の場合、UCPAの「利用内容11」およびPTA-1を選択する操作を、図示せぬ操作部に対して行う。これにより、入力制御部6 8は、ユーザの操作に対応する信号（UCPAの「利用内容11」のIDとPTA-1のID）を操作部から受信し、それをSAM 6 2に出力する。SAM 6 2の課金モジュール7 2は、入力制御部6 8からのUCPAの「利用内容11」のIDとPTA-1のIDに基づいて、UCSAおよび課金情報Aを作成する。

なお、この例の場合、レシーバ3 0 1は、UCPやPTの内容を表示する表示部や、ユーザが、利用内容等を選択することができる操作部を有していない。そこで、このように、レシーバ3 0 1に接続され、表示部および操作部を有するレシーバ5 1を利用して、ユーザは、UCPの内容やPTを選択する。

次に、ステップS 4 0 9において、レシーバ5 1のSAM 6 2は、ステップS 4 0 8で作成した課金情報Aを記憶モジュール7 3に記憶させ、また作成したUCSAを、コンテンツ鍵K c o A、およびその署名とともに一時鍵K t e m pで暗号化し、レシーバ3 0 1に送信する。なお、この処理が実行されるタイミングで、HDD 5 2に記憶されているコンテンツAも一時鍵K t e m pで暗号化され、レシーバ3 0 1に送信される。また、レシーバ5 1は、UCSAおよびコンテンツ鍵K c o Aを、レシーバ3 0 1に送信した後、消去（破棄）する。これにより、コンテンツAを利用する権利は、レシーバ3 0 1のみにより保持されるようになる。

次に、ステップS 4 1 0において、レシーバ3 0 1のSAM 3 1 1は、ステップS 4 0 9でレシーバ5 1から送信されてきたUCSA、コンテンツ鍵K c o A、およびその署名、並びにコンテンツAを受信し、一時鍵K t e m pで復号する。ステップS 4 1 1において、レシーバ3 0 1の復号／暗号化モジュール3 2 4は、ステップS 4 1 0で受信された署名を確認し、レシーバ5 1から送信されてきたデータが改竄されているか否かを判定する。この署名の確認は、図3 7のステップS 8 3における処理と同様であるので、その説明は省略する。

ステップS 4 1 1において、レシーバ5 1から送信されてきたデータが改竄されていないと判定した場合、ステップS 4 1 2に進み、レシーバ3 0 1のSAM 3 1 1は、ステップS 4 1 0で受信されたUCSA、コンテンツ鍵K c o A、およびコンテンツAを外部記憶部3 1 2の利用情報記憶部3 1 2 Aの、ステップS 4 0 5で検出されたブロックBPに記憶させる。

次に、ステップS 4 1 3において、レシーバ3 0 1のデータ検査モジュール3 2 5は、ステップS 4 1 2で、UCSA、コンテンツ鍵K c o A、およびコンテンツAが記憶された外部記憶部3 1 2の利用情報記憶部3 1 2 AのブロックBPのデータにハッシュ関数を適用して、ハッシュ値を算出する。そして、ステップS 4 1 4において、データ検査モジュール3 2 5は、算出したハッシュ値を、記憶モジュール3 2 3に記憶されている、ブロックBPに対応する検査値HPに上

書きする。

ステップS 4 0 2において、登録リストが改竄されていると判定された場合、ステップS 4 0 3において、レシーバ3 0 1が代理決済すべき機器でないと判定された場合、およびステップS 4 0 6において、検出されたブロックBP が改竄されていると判定された場合、処理は終了される。

ステップS 4 1 1において、レシーバ5 1からのデータが改竄されていると判定された場合、ステップS 4 1 5に進み、レシーバ3 0 1のSAM3 1 1は、その旨をレシーバ5 1に通知する等の処理を実行する。その後、ステップS 4 0 9に戻る。すなわち、これにより、UCSA、コンテンツ鍵K c o A、およびその署名、並びにコンテンツAが、再度、レシーバ3 0 1に送信される。なお、この例の場合、レシーバ5 1からの、この送信は、予め決められた回数だけ行われるものとし、その回数を越えた場合、処理は終了されるものとする。また、これにより処理が終了された場合、ステップS 4 0 9で、レシーバ5 1の記憶モジュール7 3に記憶された課金情報Aを削除するようにすることもできるが、課金情報Aに代理購入処理が成功しなかった（失敗した）回数を設定するようにして、その代理購入処理の失敗回数が所定の回数を超えた場合、登録リストの、レシーバ3 0 1のSAM3 1 1のIDに対応する「状態フラグ」に“制限あり”とし、レシーバ3 0 1において行われる処理を制限するようにすることもできる。

以上のようにして、レシーバ5 1により、レシーバ3 0 1に対する、コンテンツの代理購入が行われるが、課金情報は、レシーバ3 0 1に供給されずに、レシーバ5 1に保持されているので、ここで計上された課金は、レシーバ5 1自身の課金として精算される（図4 2のフローチャートにより決済される）。

次に、レシーバ3 0 1が複数のコンテンツを購入する場合の、レシーバ5 1による代理購入処理の処理手順を、図6 0のフローチャートを参照して説明する。ステップS 4 3 1において、レシーバ3 0 1と相互認証を行う。この相互認証は、図3 7を参照して説明した場合と同様であるので、その説明は省略するが、これにより、レシーバ5 1の相互認証モジュール7 1は、レシーバ3 0 1のSAM

311のIDを取得し、レシーバ301と一時鍵Ktempを共有する。

ステップS432乃至S434においては、図59のステップS402乃至S404における場合と同様の処理が実行されるので、その説明は省略する。

ステップS435において、レシーバ301のSAM311は、カウンタjの値を初期値1に設定し、次に、レシーバ301のデータ検査モジュール325は、コンテンツj(=1, 2, 3...K)を記憶する、外部記憶部312の利用情報記憶部311AのブロックBPを検出する。

ステップS437乃至S446においては、図59のステップS406乃至S415における場合と同様の処理が実行されるので、その説明は省略する。

ステップS447において、レシーバ301のSAM311は、カウンタjの値が、購入したいコンテンツの数Kと一致するか否かを判定し、一致しない場合、ステップS448に進み、カウンタjの値を1だけ増加させ、ステップS436に戻る。これにより、次の、代理購入されるコンテンツjに対応する処理が実行される。

ステップS447で、カウンタjの値が、代理するコンテンツの数Kと等しいと判定された場合、処理は終了される。

以上のようにして、複数のコンテンツが代理購入される。

次に、レシーバ301が、複数のコンテンツを購入する場合の、レシーバ51による代理購入処理の他の手順を、図61のフローチャートを参照して説明する。この例の場合も、図60における場合と同様に、レシーバ301が、K個のコンテンツを購入するものとする。

ステップS461において、レシーバ51は、レシーバ301と相互認証を行う。この相互認証は、図37を参照して説明した場合と同様であるので、その説明は省略するが、これにより、レシーバ51の相互認証モジュール71は、レシーバ301のSAM311のIDを取得し、レシーバ301と一時鍵Ktempを共有する。

ステップS462, S463においては、図59のステップS402、S40

3における場合と同様の処理が実行されるので、その説明は省略する。

ステップS 4 6 3において、レシーバ3 0 1が、代理購入することができる機器であると判定した場合、レシーバ5 1のSAM 6 2は、コンテンツを記憶することができる記憶容量の通知を要求する所定の信号を、レシーバ3 0 1に送信する。

レシーバ5 1から送信された、記憶容量の通知を要求する信号を受信すると、ステップS 4 6 5において、レシーバ3 0 1のSAM 3 1 1は、コンテンツを記憶することができる、いわゆる、空いている、外部記憶部3 1 2の利用情報記憶部3 1 2 A（ブロックBP）の記憶容量を調査し、それをレシーバ5 1に通知する。

ステップS 4 6 6において、レシーバ5 1は、ステップS 4 6 5で通知された記憶容量に記憶することができる $k$ （ $= < K$ ）個のコンテンツのIDを、レシーバ3 0 1に通知する。例えば、通知されたレシーバ3 0 1の外部記憶部3 1 2の空いている容量が、十分大きい場合、購入したい $K$ 個のコンテンツの全てのIDが通知され、またその容量が十分大きくない場合、その容量に記憶することができる分だけのコンテンツのIDが通知される。

ステップS 4 6 7において、レシーバ3 0 1のデータ検査モジュール3 2 5は、ステップS 4 6 6でIDが通信された $k$ 個のコンテンツを記憶する、外部記憶部3 1 2の利用情報記憶部3 1 2 Aの $k$ 個のブロックBPを検出する。ステップS 4 6 8において、レシーバ3 0 1のデータ検査モジュール3 2 5は、ステップS 4 6 7で検出した利用情報記憶部3 1 2 Aの $k$ 個のブロックBPのそれぞれのデータにハッシュ関数を適用してハッシュ値を算出し、記憶モジュール3 2 3に記憶されている、検出された $k$ 個のブロックBPに対応する検査値HPと一致しているか否かをそれぞれ判定し、 $k$ 個のブロックBPのデータが改竄されているか否かを判定する。

ステップS 4 6 8において、ステップS 4 6 7で検出された全てのブロックBPのデータが改竄されていないと判定された場合、ステップS 4 6 9に進み、レ

シーバ301のSAM311は、ステップS466でIDが通知されたk個のコンテンツを受け取ることが可能であることを示す信号を、通信部314を介して、レシーバ51に送信する。

ステップS470において、レシーバ51のSAM62（課金モジュール72）は、k個のコンテンツに対応するk個のUCSおよびk個の課金情報を作成する。なお、ここでの具体的な処理は、図59のステップS408における場合と、基本的に同様であるので、その説明は省略する。

次に、ステップS471において、レシーバ51のSAM62は、作成したk個の課金情報を記憶モジュール73に記憶させ、また作成したk個のUCSを、k個のコンテンツ鍵Kco、およびその署名とともに一時鍵Ktempで暗号化し、レシーバ301に送信する。なお、この処理が実行されるタイミングで、HDD52に記憶されているk個のコンテンツ（購入される）も一時鍵Ktempで暗号化され、レシーバ301に送信される。

次に、ステップS472において、レシーバ301のSAM311は、ステップS471でレシーバ51から送信されてきたk個のUCS、k個のコンテンツ鍵Kco、および署名、並びにk個のコンテンツをデータを受信し、一時鍵Ktempで復号する。ステップS473において、レシーバ301の復号／暗号化モジュール324は、ステップS472で受信された署名を確認し、レシーバ51から送信されてきたデータが改竄されているか否かを判定する。この署名の確認は、図37のステップS83における処理と同様であるので、その説明は省略する。

ステップS473において、レシーバ51から送信されてきたデータが改竄されていないと判定された場合、ステップS474に進み、レシーバ301のSAM311は、ステップS472で受信されたk個のUCS、k個のコンテンツ鍵Kco、およびk個のコンテンツを外部記憶部312の利用情報記憶部312Aの、ステップS467で検出されたk個のブロックBPに記憶させる。

ステップS475において、レシーバ301のデータ検査モジュール325は

、ステップS 4 7 4で、UCS、コンテンツ鍵K c o、およびコンテンツが記憶された外部記憶部3 1 2の利用情報記憶部3 1 2 Aのk個のブロックBPのデータにハッシュ関数を適用して、それぞれのハッシュ値を算出し、それを、ステップS 4 7 6において、記憶モジュール3 2 3に記憶されている、対応する検査値HPに上書きする。その後、処理は終了される。

ステップS 4 6 2において、登録リストが改竄されていると判定された場合、ステップS 4 6 3において、レシーバ3 0 1が代理決済すべき機器でないと判定された場合、およびステップS 4 6 8において、検出されたブロックBPが改竄されていると判定された場合、処理は終了される。

ステップS 4 7 3において、レシーバ5 1からのデータが改竄されていると判定された場合、ステップS 4 7 7に進み、レシーバ3 0 1のSAM3 1 1は、その旨をレシーバ5 1に通知する等の処理を実行する。その後、ステップS 4 7 1に戻る。すなわち、これにより、k個のUCS、k個のコンテンツ鍵K c o、およびその署名、並びにk個のコンテンツが、再度、レシーバ3 0 1に送信される。なお、この場合も、レシーバ5 1からの、この送信は、予め決められた回数だけ行われるものとし、その回数を越えた場合、処理は終了されるものとする。また、これにより処理が終了された場合、ステップS 4 7 1で、レシーバ5 1の記憶モジュール7 3に記憶されたk個の課金情報を削除するようにすることもできるが、k個の課金情報のそれぞれに代理購入処理の失敗回数を設定するようにして、その回数が所定の回数を越えた場合、登録リストの、レシーバ3 0 1のSAM3 1 1のIDに対応する「状態フラグ」に” 制限あり” とし、レシーバ3 0 1において行われる処理を制限することもできる。

次に、レシーバ5 1が、レシーバ4 0 1に代わり、コンテンツを購入する場合（代理購入する場合）の処理手順を、図6 2，図6 3のフローチャートを参照して説明する。レシーバ5 1は、レシーバ4 0 1から、購入したいコンテンツのIDと、所定の代理購入を依頼する所定の信号を受信すると、ステップS 5 0 1において、レシーバ5 1は、レシーバ4 0 1と相互認証を行う。この相互認証は、

図37を参照して説明した場合と同様であるので、その説明は省略するが、これにより、レシーバ51の相互認証モジュール71は、レシーバ401のSAM411のIDを取得し、レシーバ401と一時鍵Ktempを共有する。

ステップS502において、レシーバ51のSAM62は、HDD52に記憶されている登録リストが改竄されているか否かを判定し、登録リストが改竄されていないと判定された場合、ステップS503に進み、代理購入の依頼のあったレシーバ401が、代理購入すべき機器であるか否かを判定する。ここでの具体的な処理は、図59のステップS403における場合と同様であるので、その説明は省略する。ステップS503で、レシーバ401が、代理決済すべき機器であると判定した場合、レシーバ51のSAM62は、ステップS504に進み、予め通知された、レシーバ501が購入したいコンテンツのUCPおよびPTを、署名を付して、レシーバ401に送信する。なお、UCP、PT、およびコンテンツは、サービスプロバイダセキュアコンテナに含まれているので、そのまま渡してもよい。

ステップS505において、レシーバ401のSAM411は、レシーバ51から送信されたUCP、PT、およびその署名を受信し、ステップS506において、署名を確認し、レシーバ51から送信されてきたデータが改竄されているか否かを判定する。この署名の確認は、図37のステップS83における処理と同様であるので、その説明は省略する。

ステップS506において、レシーバ51から送信されてきたデータが改竄されていないと判定した場合、レシーバ401のSAM411は、ステップS507に進み、購入するコンテンツに対応するコンテンツ鍵Kcoを記憶する、外部記憶部412の利用情報記憶部412AのブロックBP（図示せず）を検出する。

次に、ステップS508において、レシーバ401のデータ検査モジュール425は、ステップS507で検出された利用情報記憶部412AのブロックBPに記憶されているデータの全体にハッシュ関数を適用してハッシュ値を算出し、

記憶モジュール 4 2 3 に記憶されている、検出されたブロック B P に対応する検査値 H P と一致するか否かを判定する。それらの値が一致すると判定された場合、すなわち、利用情報記憶部 4 1 2 A の、検出されたブロック B P が改竄されていない場合、ステップ S 5 0 9 に進む。

ステップ S 5 0 9 において、レシーバ 4 0 1 の S A M 4 1 1 は、ステップ S 5 0 5 で受信された U C P の「利用内容」と P T の I D をレシーバ 5 1 の通知する。なお、実際は、この処理に先だって、レシーバ 4 0 1 の表示制御部 4 1 6 が、ステップ S 5 0 5 で受信された U C P および P T の内容を、図示せぬ表示部に出力し、ユーザに提示する。ユーザは、提示されたこれらの情報から、U C P の利用内容および P T を選択する操作を、図示せぬ操作部に対して行う。これにより、入力制御部 4 1 7 は、ユーザの操作に対応する信号（U C P の「利用内容」の I D と P T の I D）を操作部から受信し、それを S A M 4 1 1 に出力する。S A M 4 1 1 は、入力制御部 4 1 7 からの情報を、通信部 4 1 4 に介してレシーバ 5 1 に送信する。

このように、ユーザが、U C P の内容および P T を選択することができる機能を有するレシーバ 4 0 1 に対しては、U C P および P T（購入するコンテンツの I D および選択項目）が、レシーバ 5 1 から送信される。なお、U C P および P T に代えて、ステップ S 5 1 0 において、レシーバ 5 1 の S A M 6 2 は、レシーバ 4 0 1 から通知された U C P の「利用内容」の I D および P T の I D（購入するコンテンツの I D および選択項目）に基づいて、課金情報および U C S を作成する。次に、ステップ S 5 1 1 において、レシーバ 5 1 の S A M 6 2 は、ステップ S 5 1 0 で作成した課金情報を記憶モジュール 7 3 に記憶させ、そして作成した U C S を、購入されるコンテンツに対応するコンテンツ鍵 K c o、およびそれらの署名とともにレシーバ 4 0 1 に送信する。なお、この処理が実行されるタイミングで、H D D 5 2 に記憶されている、購入されるコンテンツもレシーバ 4 0 1 に送信される。なお、サービスプロバイダセキュアコンテナをレシーバ 4 0 1 に送信し、レシーバ 4 0 1 が、改竄チェック、利用内容の選択、および要求を

出して、レシーバ51で購入し、UCSや鍵を渡すようにすることもできる。

次に、ステップS512において、レシーバ401のSAM411は、ステップS511でレシーバ51から送信されてきたUCS、コンテンツ鍵Kco、およびその署名、並びにコンテンツを受信し、一時鍵Ktempで復号する。ステップS513において、レシーバ401の復号/暗号化モジュール424は、ステップS512で受信された署名を確認し、レシーバ51から送信されてきたデータが改竄されているか否かを判定する。この署名の確認は、図37のステップS83における処理と同様であるので、その説明は省略する。

ステップS513において、レシーバ51から送信されてきたデータが改竄されていないと判定された場合、ステップS514に進み、レシーバ401のSAM411は、ステップS505で受信されたUCP、PT、およびコンテンツをHDD402に記憶させる。次に、ステップS515において、SAM411は、ステップS512で受信されたUCSとコンテンツ鍵Kcoを、外部記憶部412の利用情報記憶部412Aの、ステップS507で検出されたブロックBPに記憶させる。

次に、ステップS516において、レシーバ401のデータ検査モジュール425は、ステップS515で、UCSとコンテンツ鍵Kcoが記憶された外部記憶部412の利用情報記憶部412AのブロックBPのデータにハッシュ関数を適用して、ハッシュ値を算出し、それを、ステップS517において、記憶モジュール423に記憶されている、対応する検査値HPに上書きする。

ステップS502において、登録リストが改竄されていると判定された場合、ステップS503において、レシーバ401が代理決済すべき機器でないと判定された場合、およびステップS508において、利用情報が記憶されるブロックBPが改竄されていると判定された場合、処理は終了される。

ステップS506において、レシーバ51からのデータが改竄されていると判定された場合、ステップS518に進み、レシーバ401のSAM411は、その旨をレシーバ51に通知する等の処理を実行する。その後、ステップS504

に戻る。すなわち、これにより、UCP、PT、およびその署名が、再度、レシーバ401に送信される。なお、この例の場合、レシーバ51からの、この送信は、予め決められた回数だけ行われるものとし、その回数を越えた場合、処理は終了されるものとする。

ステップS513において、レシーバ51からのデータが改竄されていると判定された場合、ステップS519に進み、レシーバ401のSAM411は、その旨をレシーバ51に通知する等の処理を実行する。その後、ステップS511に戻る。すなわち、これにより、UCS、コンテンツ鍵Kco、およびその署名、並びにコンテンツが、再度、レシーバ401に送信される。なお、この例の場合、レシーバ51からの、この送信は、予め決められた回数だけ行われるものとし、その回数を越えた場合、処理は終了されるものとする。また、これにより終了された場合、ステップS510で、レシーバ51の記憶モジュール73に記憶された課金情報を削除するようにすることもできるが、課金情報に代理購入処理の失敗回数を設定するようにして、その回数が所定の回数を越えたとき、登録リストのレシーバ401のSAM411のIDに対応する「状態フラグ」に”制限あり”とし、レシーバ401における処理を制限するようにすることもできる。

なお、コンテンツは、音楽データを例に説明したが、音楽データに限らず、動画像データ、静止画像データ、文書データ、またはプログラムデータでもよい。その際、圧縮は、コンテンツの種類に適した方式、例えば、画像であればMPEG (Moving Picture Experts Group) などが利用される。ウォーターマークも、コンテンツの種類に適した形式のウォーターマークが利用される。

また、共通鍵暗号は、ブロック暗号であるDESを使用して説明したが、NTT (商標) が提案するFEAL、IDEA (International Data Encryption Algorithm)、または1ビット乃至数ビット単位で暗号化するストリーム暗号などでもよい。

さらに、コンテンツおよびコンテンツ鍵Kcoの暗号化は、共通鍵暗号方式を

利用するとして説明したが、公開鍵暗号方式でもよい。

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

上述の本発明の実施の形態のレシーバ51は、他のレシーバから、課金情報を受信し、管理装置に送信するようにしたので、他のレシーバに代わって決済処理を行うことができる。

また、本発明の実施の形態のレシーバは、代理購入情報に対応して、使用許諾条件情報を作成し、暗号化された情報を復号するために必要な鍵とともに、他の情報処理装置に送信するようにしたので、他の情報処理装置が、暗号化された情報を復号して利用することができる。

#### 産業上の利用の可能性

本発明は、音楽データ、動画データ、静止画像データ、文書データ、プログラムデータなどの情報を暗号化し、配信する情報処理システムに適應できる。

## 請 求 の 範 囲

1. 他の情報処理装置に接続され、かつ、管理装置に管理されて、暗号化された情報を復号して利用する情報処理装置において、

上記他の情報処理装置の所定の代理決済情報を記憶する記憶手段と、

上記記憶手段に記憶されている上記代理決済情報に対応して、所定の課金情報の提供を上記他の情報処理装置に要求する要求手段と、

上記要求手段による要求に応じて、上記他の情報処理装置から送信されてくる上記課金情報を受信する第1の受信手段と、

上記第1の受信手段により受信された上記課金情報を、上記管理装置に送信する送信手段と、

上記管理装置から送信されてくる、上記送信手段により送信された上記課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件を受信する第2の受信手段と、

上記第2の受信手段により受信された上記登録条件に基づいて、動作を制御する制御手段と

を具備する情報処理装置。

2. 他の情報処理装置に接続され、かつ、管理装置に管理されて、暗号化された情報を復号して利用する情報処理装置の情報処理方法において、

上記他の情報処理装置の所定の代理決済情報を記憶する記憶ステップと、

上記記憶ステップで記憶された上記代理決済情報に対応して、所定の課金情報の提供を上記他の情報処理装置に要求する要求ステップと、

上記要求ステップでの要求に応じて、上記他の情報処理装置から送信されてくる上記課金情報を受信する第1の受信ステップと、

上記第1の受信ステップで受信された上記課金情報を、上記管理装置に送信する送信ステップと、

上記管理装置から送信されてくる、上記送信ステップで送信された上記課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件を受信する第2の受信ステップと、

上記第2の受信ステップで受信された上記登録条件に基づいて、動作を制御する制御ステップと

を具備する情報処理方法。

3. 他の情報処理装置に接続され、かつ、管理装置に管理されて、暗号化された情報を復号して利用する情報処理装置に、

上記他の情報処理装置の所定の代理決済情報を記憶する記憶ステップと、

上記記憶ステップで記憶された上記代理決済情報に対応して、所定の課金情報の提供を上記他の情報処理装置に要求する要求ステップと、

上記要求ステップでの要求に応じて、上記他の情報処理装置から送信されてくる上記課金情報を受信する第1の受信ステップと、

上記第1の受信ステップで受信された上記課金情報を、上記管理装置に送信する送信ステップと、

上記管理装置から送信されてくる、上記送信ステップで送信された上記課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件を受信する第2の受信ステップと、

上記第2の受信ステップで受信された上記登録条件に基づいて、動作を制御する制御ステップと

を具備する処理を実行させるコンピュータが読み取り可能なプログラムを提供する提供媒体。

4. 他の情報処理装置に接続され、かつ、管理装置に管理されて、暗号化された情報を復号して利用する情報処理装置において、

上記他の情報処理装置の所定の代理購入情報を記憶する第1の記憶手段と、

上記第 1 の記憶手段に記憶されている上記代理購入情報に対応して、所定の課金情報を作成する第 1 の作成手段と、

上記第 1 の記憶手段に記憶されている上記代理購入情報に対応して、所定の使用許諾条件情報を作成する第 2 の作成手段と、

上記第 1 の作成手段により作成された上記課金情報を記憶する第 2 の記憶手段と、

上記第 2 の作成手段により作成された上記使用許諾条件情報と、上記管理装置から供給された、暗号化された上記情報を復号するために必要な鍵を、上記他の情報処理装置に送信する送信手段と

を具備する情報処理装置。

5. 上記他の情報処理装置が、

所定の表示を制御する表示手段と、

所定のデータの入力を制御する入力制御手段と

を備えているとき、

上記第 1 の作成手段は、上記表示手段により制御された上記表示が参照されて、上記入力制御手段に入力されたデータに基づいて、上記課金情報を作成し、

上記第 2 の作成手段は、上記表示手段により制御された上記表示が参照されて、上記入力制御手段に制御された上記データに基づいて、上記使用許諾条件情報を作成する

請求の範囲第 4 項に記載の情報処理装置。

6. 他の情報処理装置に接続され、かつ、管理装置に管理されて、暗号化された情報を復号して利用する情報処理装置の情報処理方法において、

上記他の情報処理装置の所定の代理購入情報を記憶する第 1 の記憶ステップと

上記第 1 の記憶ステップで記憶された上記代理購入情報に対応して、所定の課

金情報を作成する第 1 の作成ステップと、

上記第 1 の記憶ステップで記憶された上記代理購入情報に対応して、所定の使用許諾条件情報を作成する第 2 の作成ステップと、

上記第 1 の作成ステップで作成された上記課金情報を記憶する第 2 の記憶ステップと、

上記第 2 の作成ステップで作成された上記使用許諾条件情報と、上記管理装置から供給された、暗号化された上記情報を復号するために必要な鍵を、上記他の情報処理装置に送信する送信ステップと

を具備する情報処理方法。

7. 他の情報処理装置に接続され、かつ、管理装置に管理されて、暗号化された情報を復号して利用する情報処理装置に、

上記他の情報処理装置の所定の代理購入情報を記憶する第 1 の記憶ステップと、

上記第 1 の記憶ステップで記憶された上記代理購入情報に対応して、所定の課金情報を作成する第 1 の作成ステップと、

上記第 1 の記憶ステップで記憶された上記代理購入情報に対応して、所定の使用許諾条件情報を作成する第 2 の作成ステップと、

上記第 1 の作成ステップで作成された上記課金情報を記憶する第 2 の記憶ステップと、

上記第 2 の作成ステップで作成された上記使用許諾条件情報と、上記管理装置から供給された、暗号化された上記情報を復号するために必要な鍵を、上記他の情報処理装置に送信する送信ステップと

を具備する処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

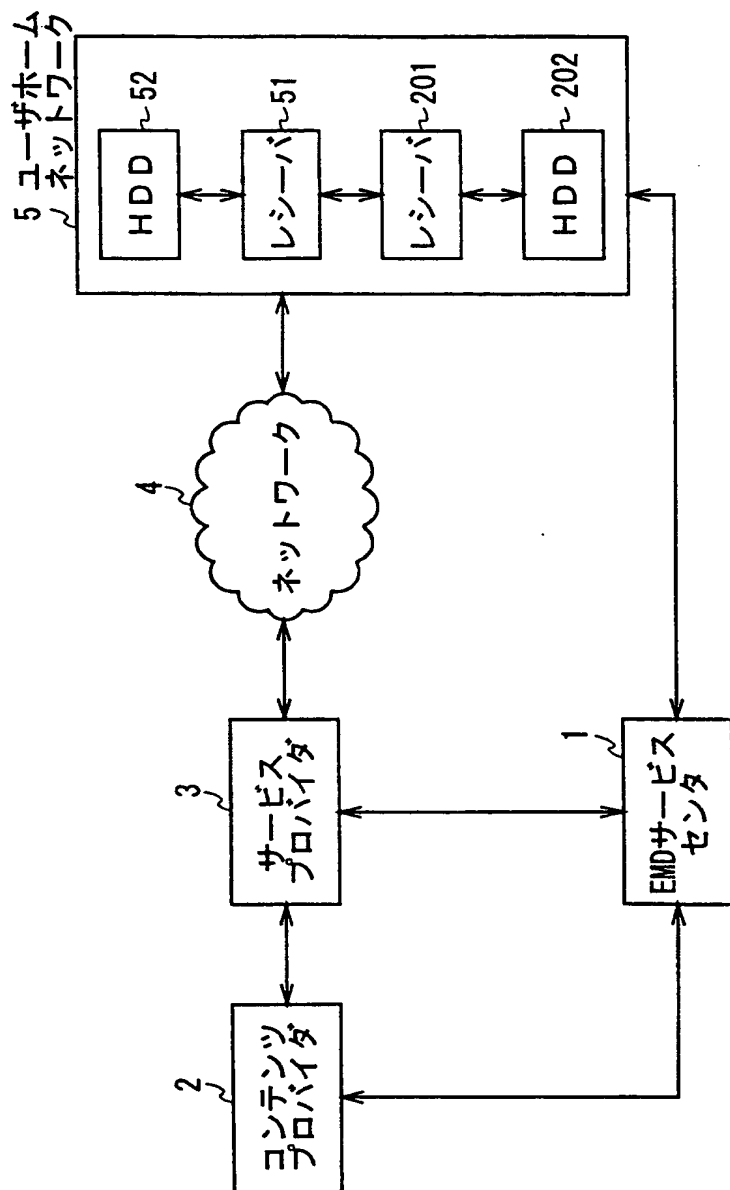


図 1

*This Page Blank (uspto)*

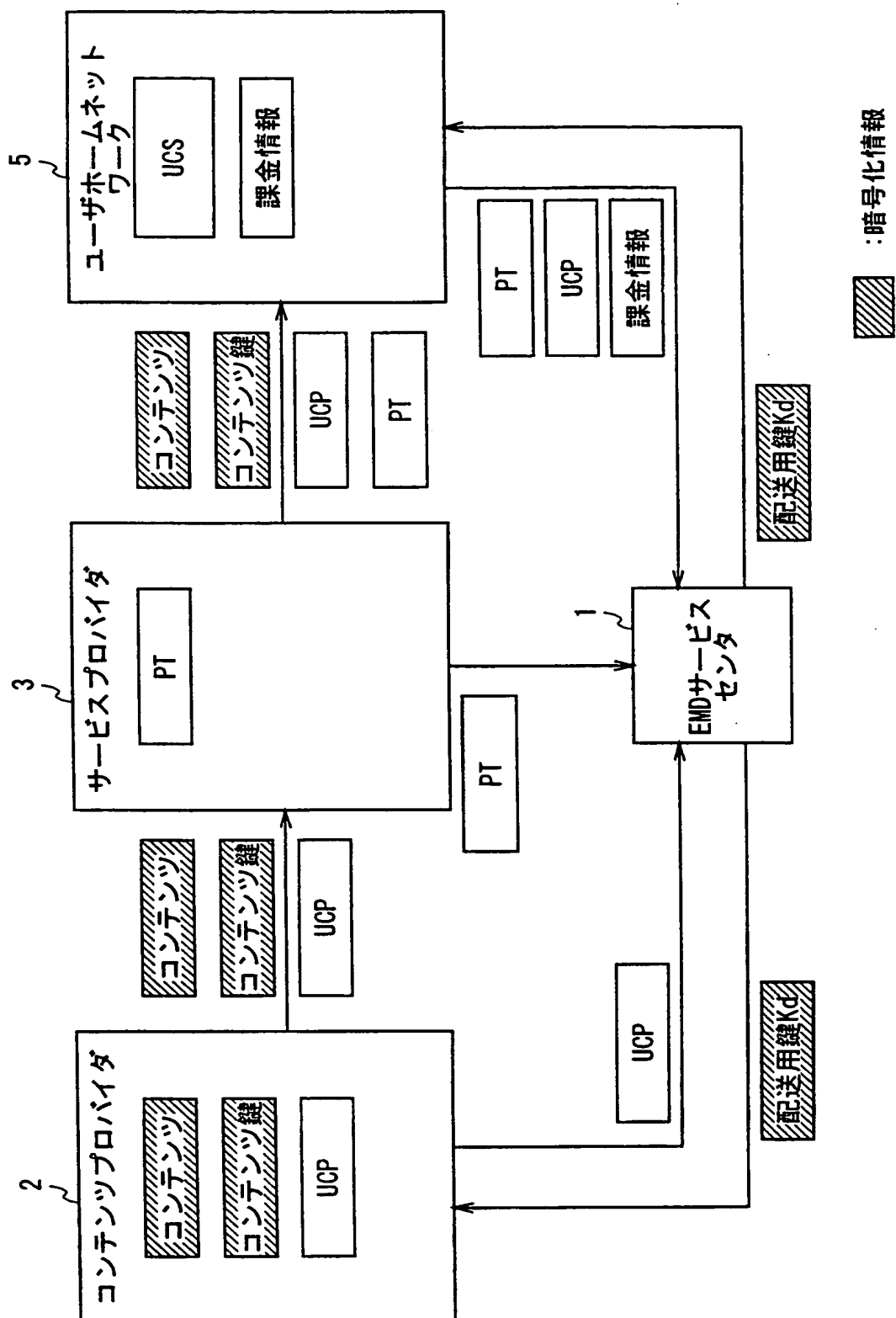
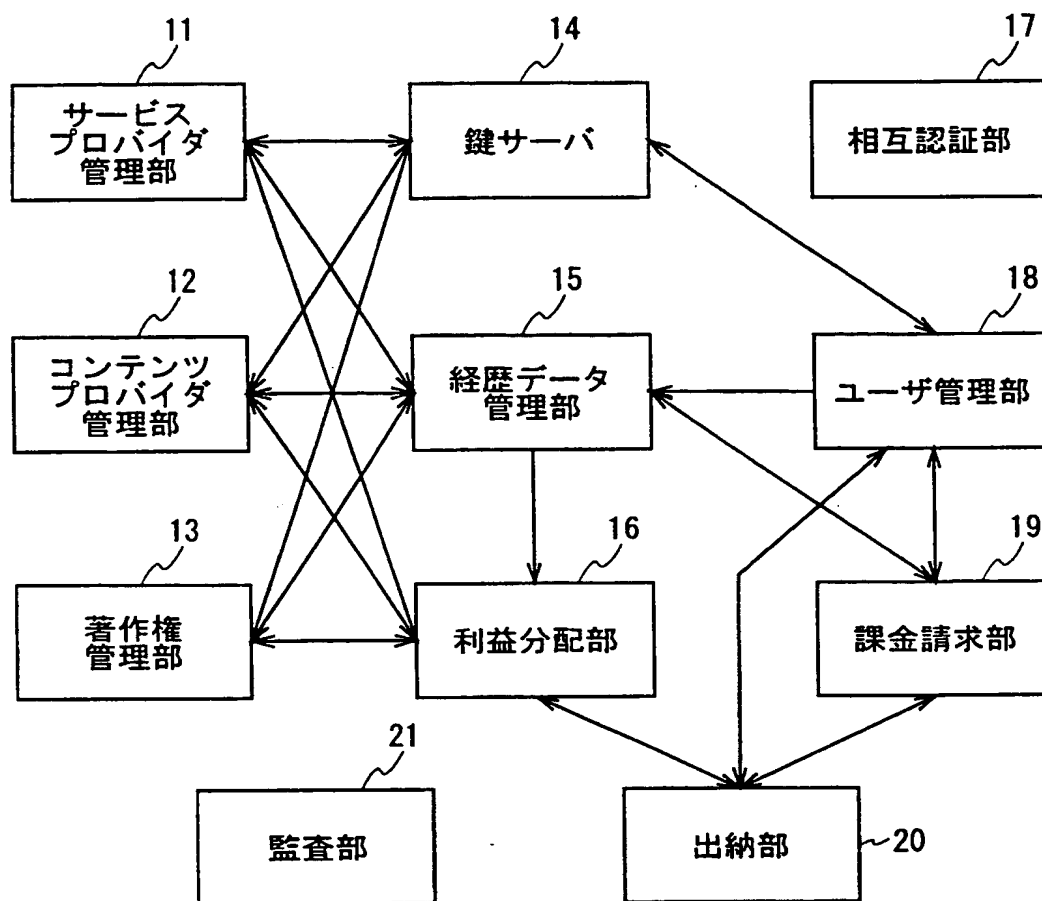


図 2

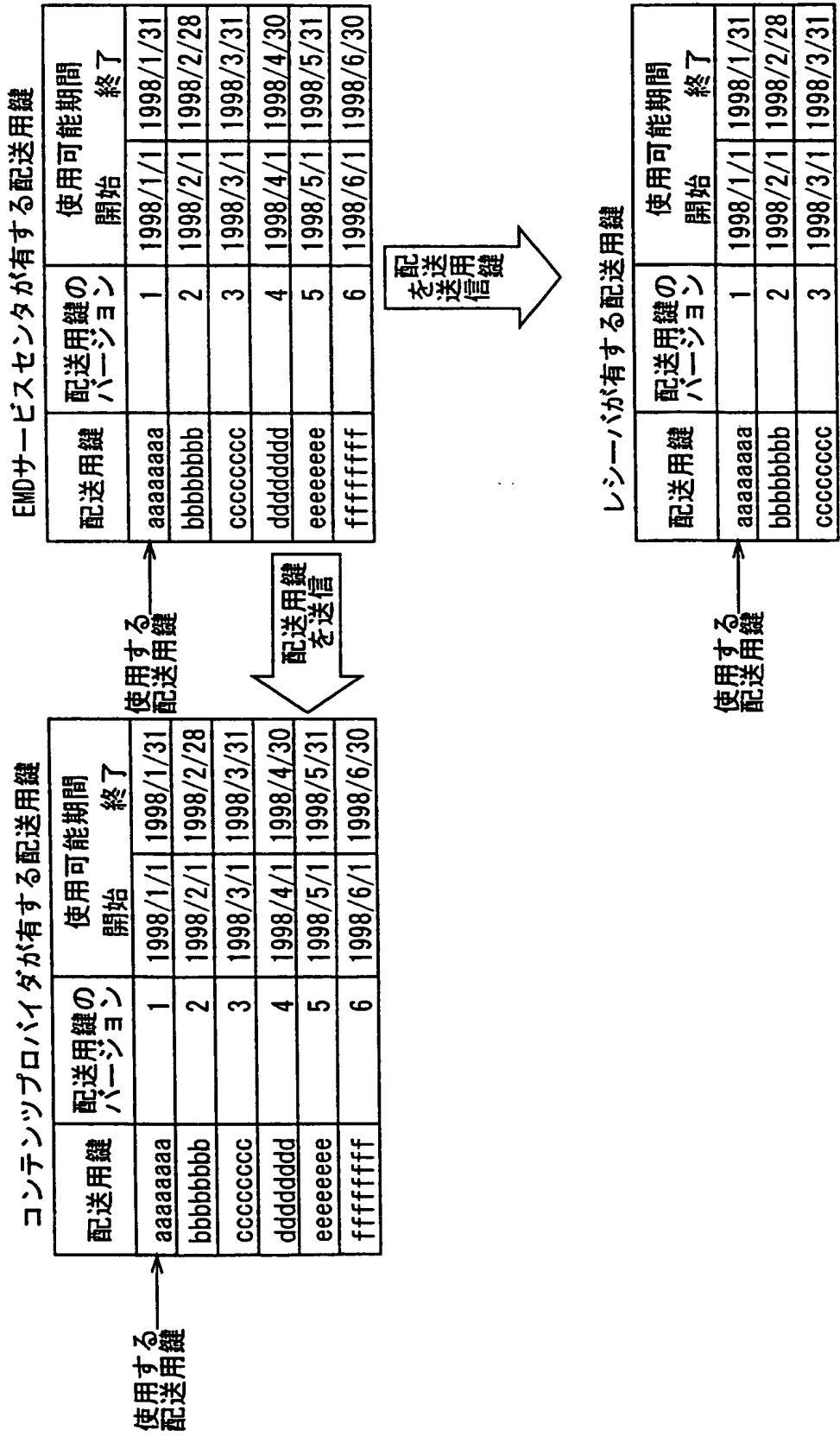
This Page Blank (uspto)



EMDサービスセンタ 1

図 3

This Page Blank (uspto)



This Page Blank (uspto)

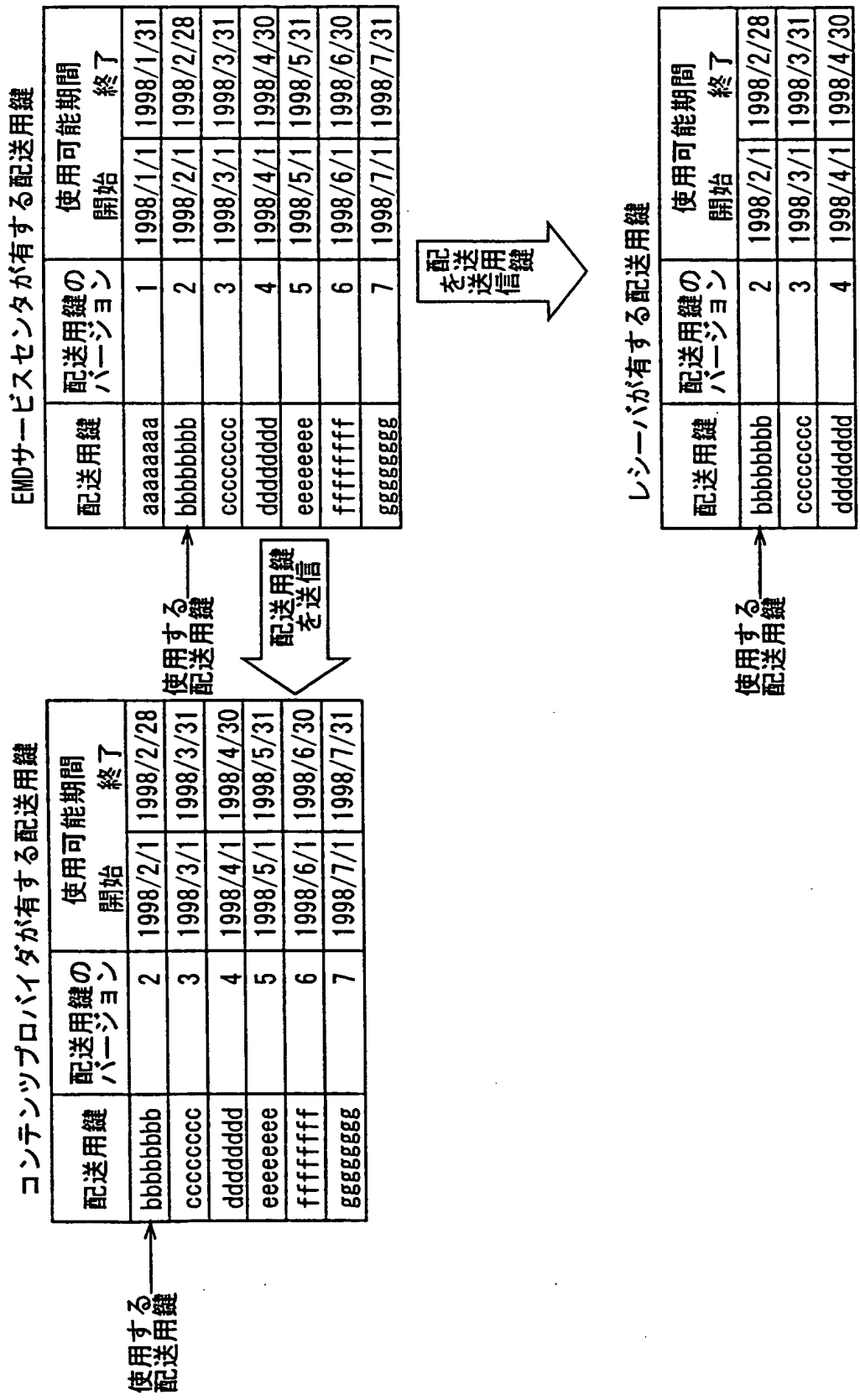


図 5

***This Page Blank (uspto)***

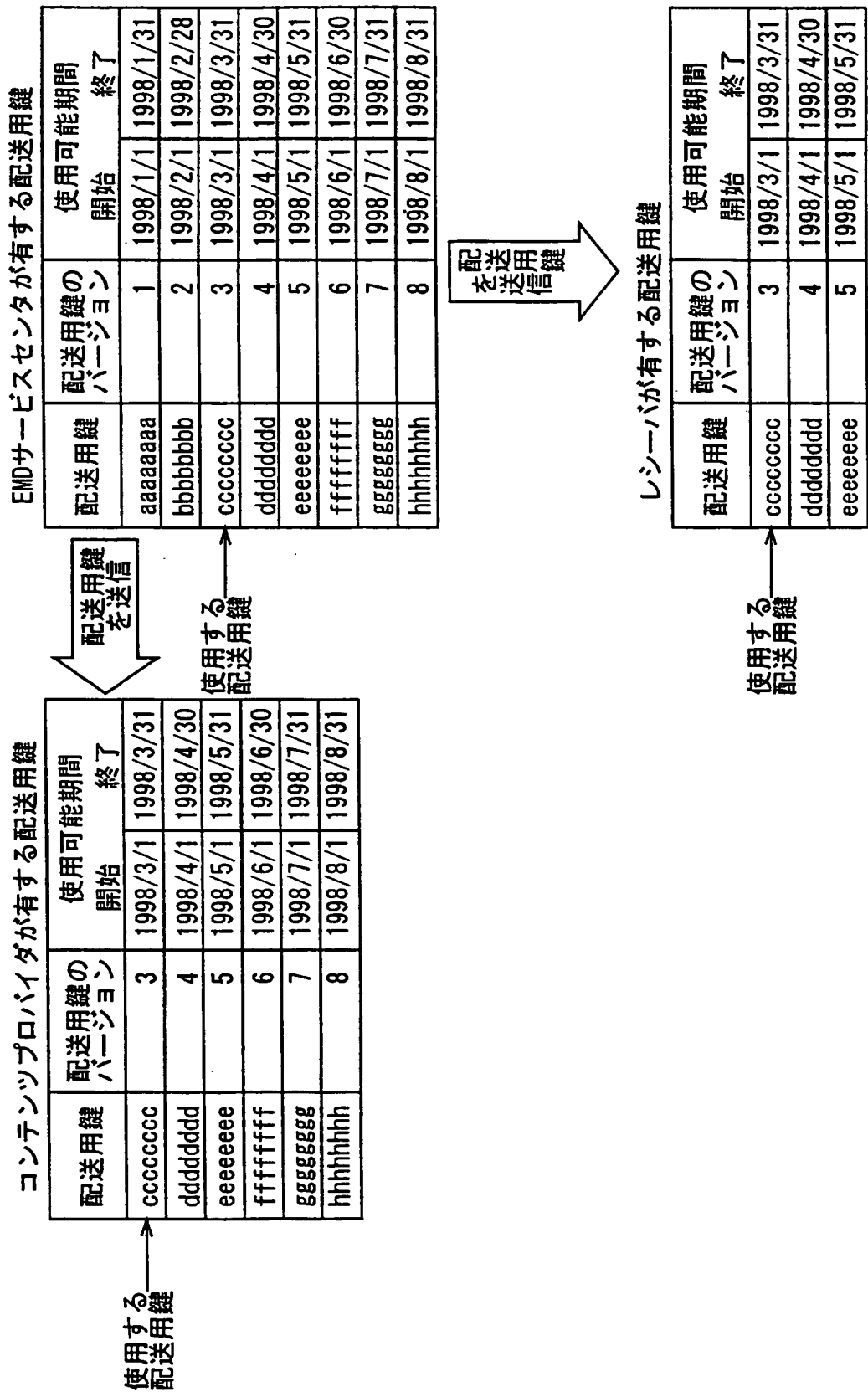


図 6

This Page Blank (uspto)

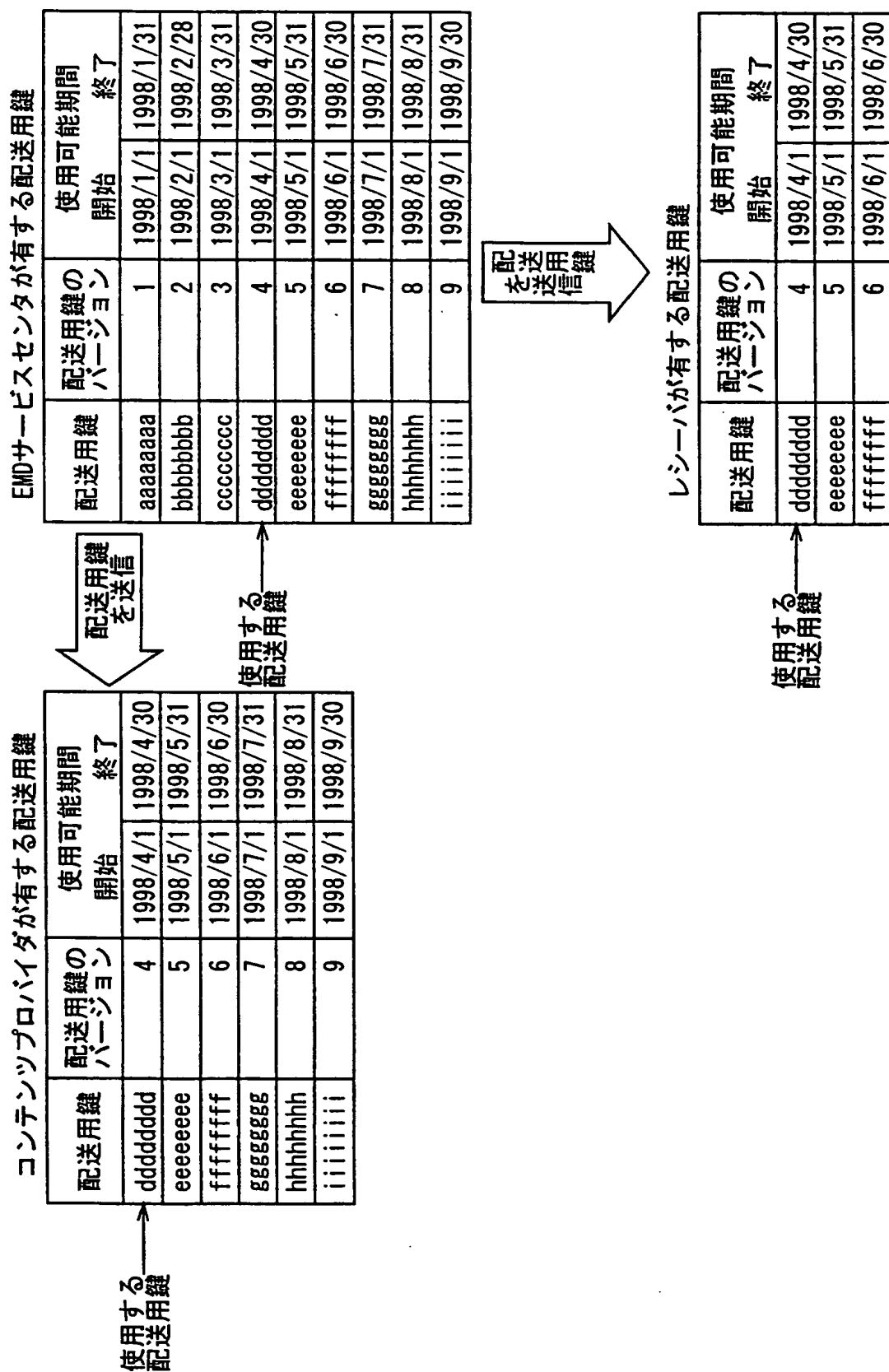
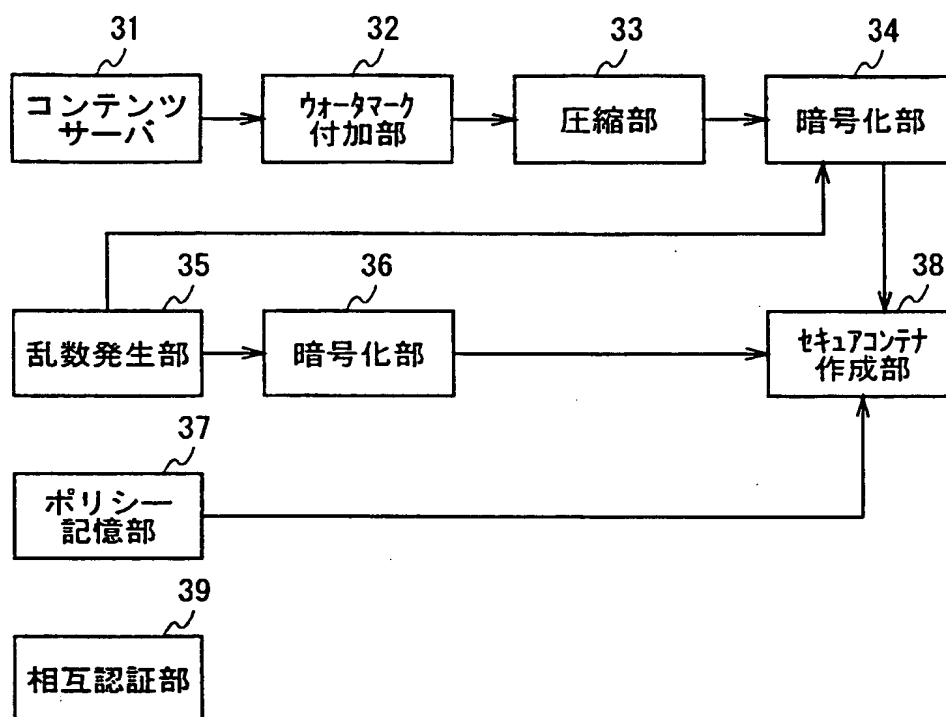


図 7

**This Page Blank (uspto)**



コンテンツプロバイダ 2

図 8

*This Page Blank (uspto)*

コンテンツのID	コンテンツAのID
コンテンツAのID	コンテンツAのID
UCPのID	UCPのID
UCPの有効期限	UCPの有効期限
利用条件 20	ユーザ条件20 200ポインタ より少ない
	機器条件20 条件なし
利用内容 21	ID 21 利用内容21のID
	形式21 Pay Per Play 4
	バージョン21 再生4回
	管理移動 許可情報21 不可
利用内容 22	ID 22 利用内容22のID
	形式22 Pay Per Copy 2
	バージョン22 複製2回
	管理移動 許可情報22 不可

UCPB

B

コンテンツのID	コンテンツAのID
コンテンツAのID	コンテンツAのID
UCPのID	UCPのID
UCPの有効期限	UCPの有効期限
利用条件 10	ユーザ条件10 200ポインタ以上
	機器条件10 条件なし
利用内容 11	ID 11 利用内容11のID
	形式11 買い取り再生
	バージョン11 x x x x x
	管理移動 許可情報11 可
利用内容 12	ID 12 利用内容12のID
	形式12 第1世代複製
	バージョン12 x x x x x
	管理移動 許可情報12 不可
利用内容 13	ID 13 利用内容13のID
	形式13 期間制限再生
	バージョン13 x x x x x
	管理移動 許可情報13 不可
利用内容 14	ID 14 利用内容14のID
	形式14 Pay Per Copy 5
	バージョン14 複製5回
	管理移動 許可情報14 不可

UCPA

図 9

A

This Page Blank (uspto)

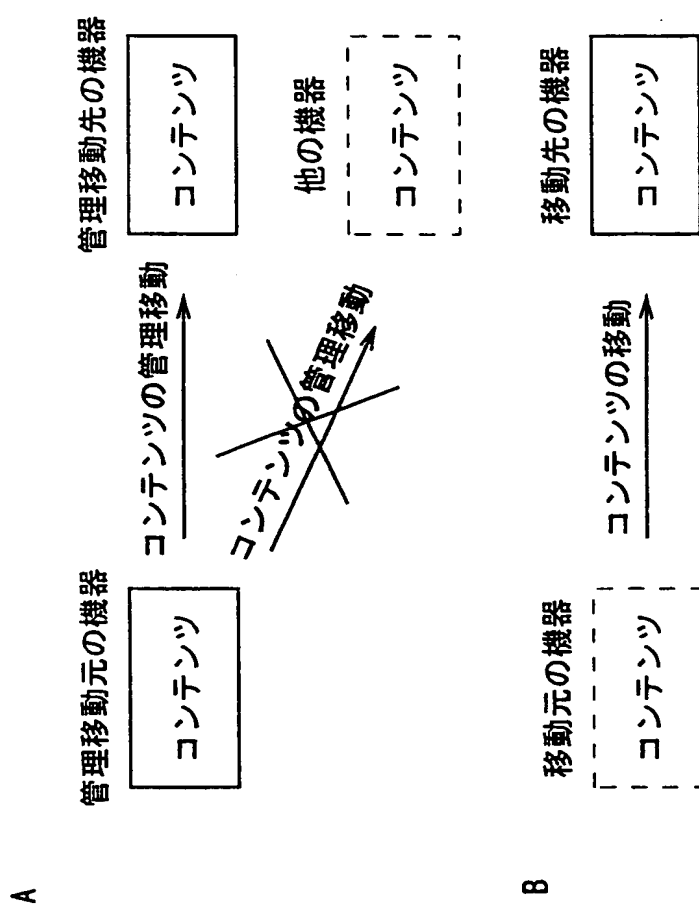
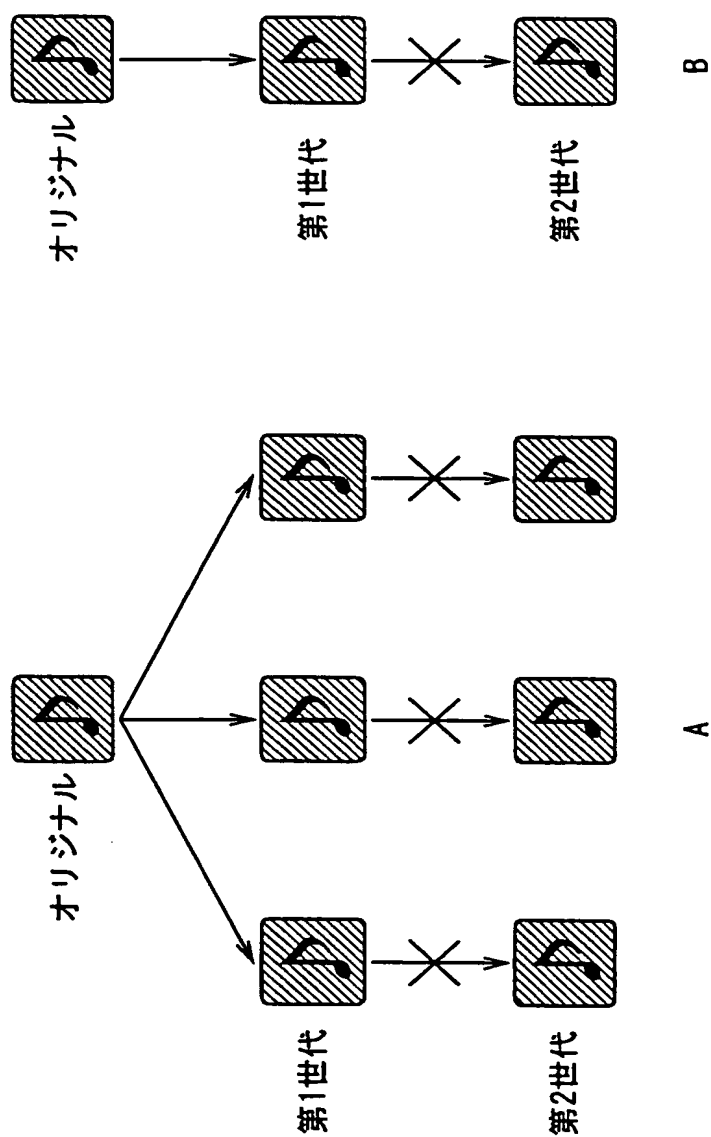


図10

**This Page Blank (uspto)**


$$\frac{1}{1-x}$$

**This Page Blank (uspto)**

## A

サービスコード	意味
0000h	条件なし
0001h乃至00FFh	機器に関し条件有り
0100h乃至01FFh	性別条件あり
0200h乃至02FFh	年令条件あり
0300h乃至7FFFh	その他の条件あり
8000h乃至FFFFh	利用ポイントに関し条件有り

## B

コンディションコード	意味
00h	無条件
01h	=
02h	≠
03h	< (より小さい)
04h	> (より大きい)
05h	≦ (以下)
06h	≧ (以上)
07h乃至FFh	空き

図 1 2

This Page Blank (uspto)

A

ユーザ条件 10	サービスコード	ハッシュコード	コンディションコード
	80 × × h	0000C8h	06h
機器条件 10	サービスコード	ハッシュコード	コンディションコード
	0000h	FFFFFFh	00h

UCPAの利用条件 10

B

ユーザ条件 20	サービスコード	ハッシュコード	コンディションコード
	80 × × h	0000C8h	03h
機器条件 20	サービスコード	ハッシュコード	コンディションコード
	0000h	FFFFFFh	00h

UCPBの利用条件 20

図 1 3

This Page Blank (uspto)

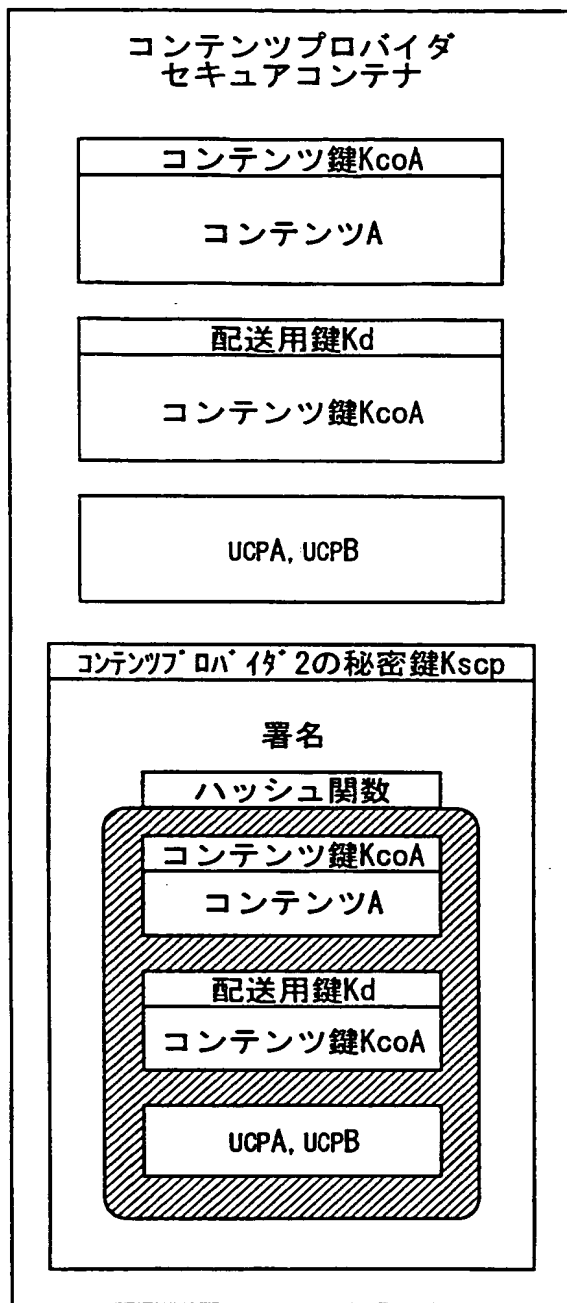


図 1 4

Best Available Copy

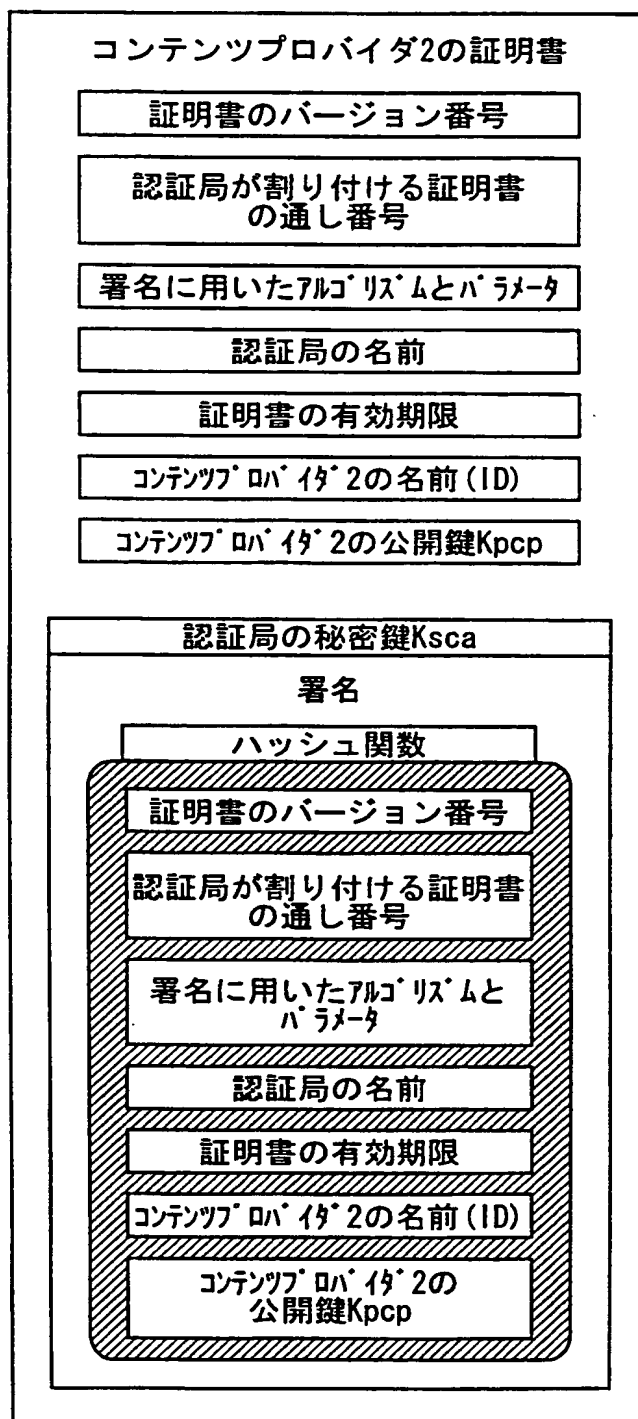


図 1 5

Best Available Copy

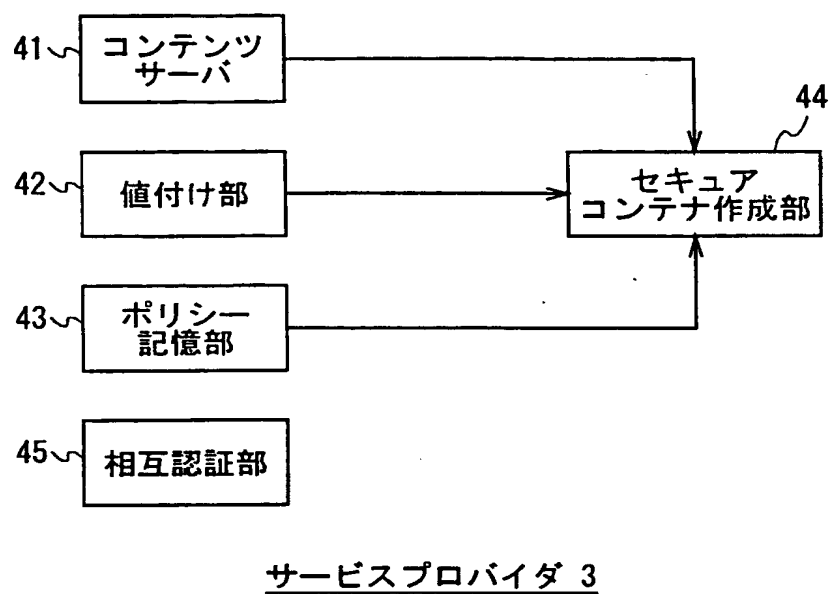


図 16

Best Available Cop,

コンテンツのID	コンテンツAのID
コンテンツIDのID	コンテンツIDのID
UCPのID	UCPAのID
UCPの有効期限	UCPAの有効期限
サービスIDのID	サービスIDのID
PTのID	PTA-2のID
PTの有効期限	PTA-2の有効期限
価格条件 20	ユーザ条件 20
	機器条件 20
価格内容 21	1000円
価格内容 22	300円
価格内容 23	50円
価格内容 24	150円

PTA-2

コンテンツのID	コンテンツAのID
コンテンツIDのID	コンテンツIDのID
UCPのID	UCPAのID
UCPの有効期限	UCPAの有効期限
サービスIDのID	サービスIDのID
PTのID	PTA-1のID
PTの有効期限	PTA-1の有効期限
価格条件 10	ユーザ条件 10
	機器条件 10
価格内容 11	2000円
価格内容 12	600円
価格内容 13	100円
価格内容 14	300円

PTA-1

図 17

Best Available Copy

A

ユーザ条件 10	サービスコード	バリュースコード	コンディションコード
	01××h	000000h	01h
機器条件 10	サービスコード	バリュースコード	コンディションコード
	0000h	FFFFFFh	00h

PTA-1の価格条件 10

B

ユーザ条件 20	サービスコード	バリュースコード	コンディションコード
	01××h	000001h	01h
機器条件 20	サービスコード	バリュースコード	コンディションコード
	0000h	FFFFFFh	00h

PTA-2の価格条件 20

図 1 8

Best Available Copy

コンテンツのID	コンテンツAのID
コンテンツID 1	コンテンツID 2のID
UCPのID	UCPのID
サブスクリプションID	サブスクリプションID 3のID
PTのID	PTB-2のID
PTの有効期限	PTB-2の有効期限
価格条件 40	ユーザ条件 40
	機器条件 40
価格内容 41	50円
価格内容 42	150円

PTB-2  
B

コンテンツのID	コンテンツAのID
コンテンツID 1	コンテンツID 2のID
UCPのID	UCPのID
サブスクリプションID	サブスクリプションID 3のID
PTのID	PTB-1のID
PTの有効期限	PTB-1の有効期限
価格条件 30	ユーザ条件 30
	機器条件 30
価格内容 31	100円
価格内容 32	300円

PTB-1  
A

図 19

Best Available Copy

A

ユーザ条件 30	サービスコード	バリユーコード	コンディションコード
	0000h	FFFFFFh	00h
機器条件 30	サービスコード	バリユーコード	コンディションコード
	00××h	000064h	03h

PTB-1の価格条件 30

B

ユーザ条件 40	サービスコード	バリユーコード	コンディションコード
	0000h	FFFFFFh	00h
機器条件 40	サービスコード	バリユーコード	コンディションコード
	00××h	000064h	06h

PTB-2の価格条件 40

図 20

Best Available Copy

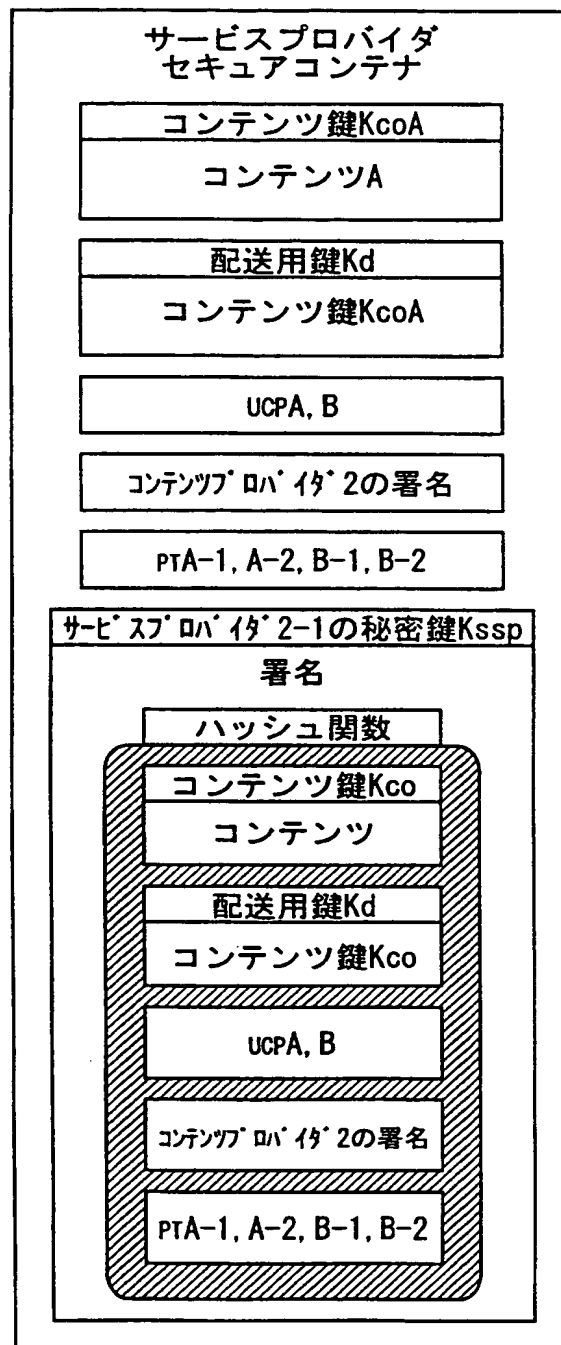


図 2 1

Best Available Copy

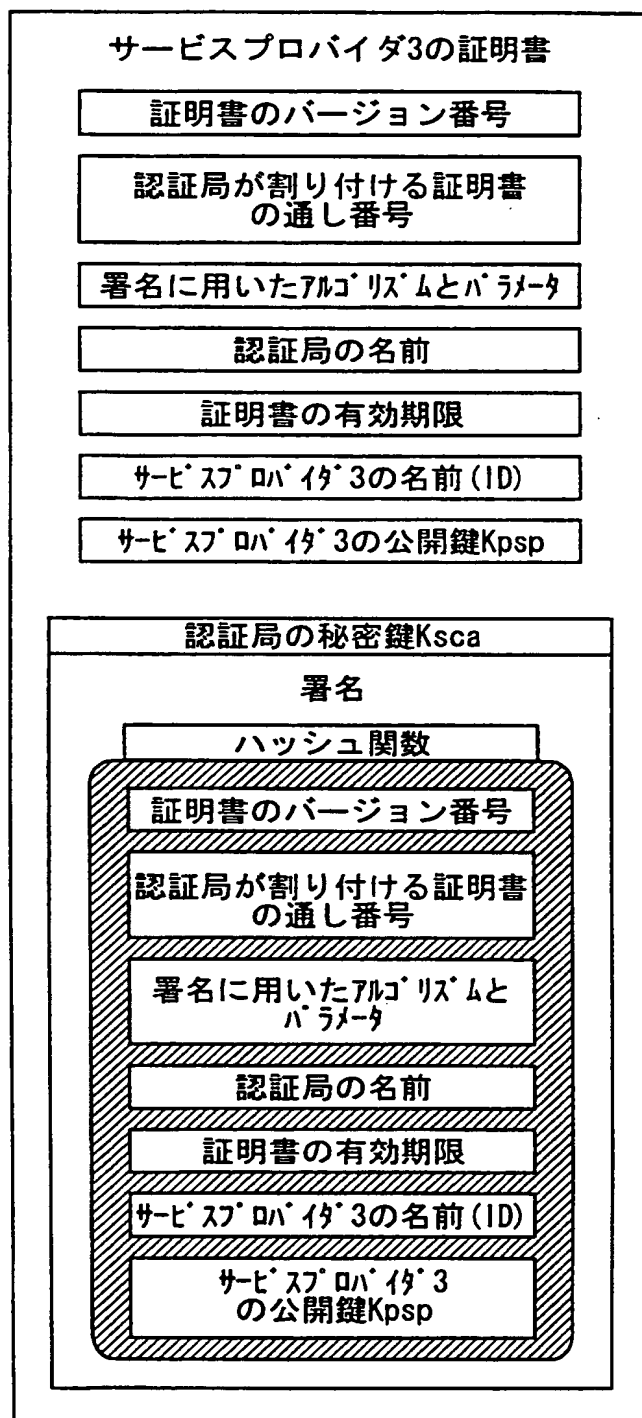


図 2 2

Best Available Copy

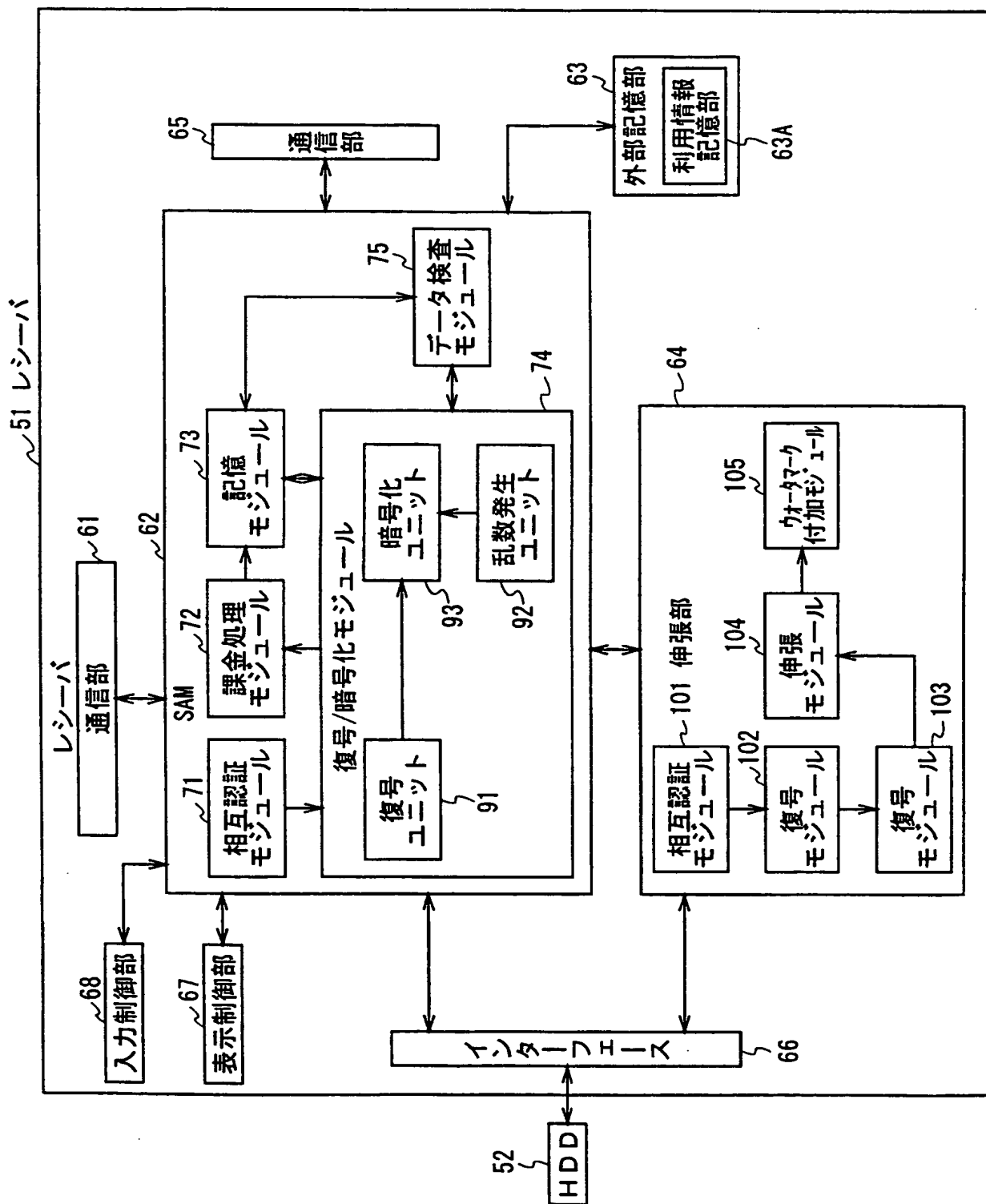


図 23

Best Available Copy

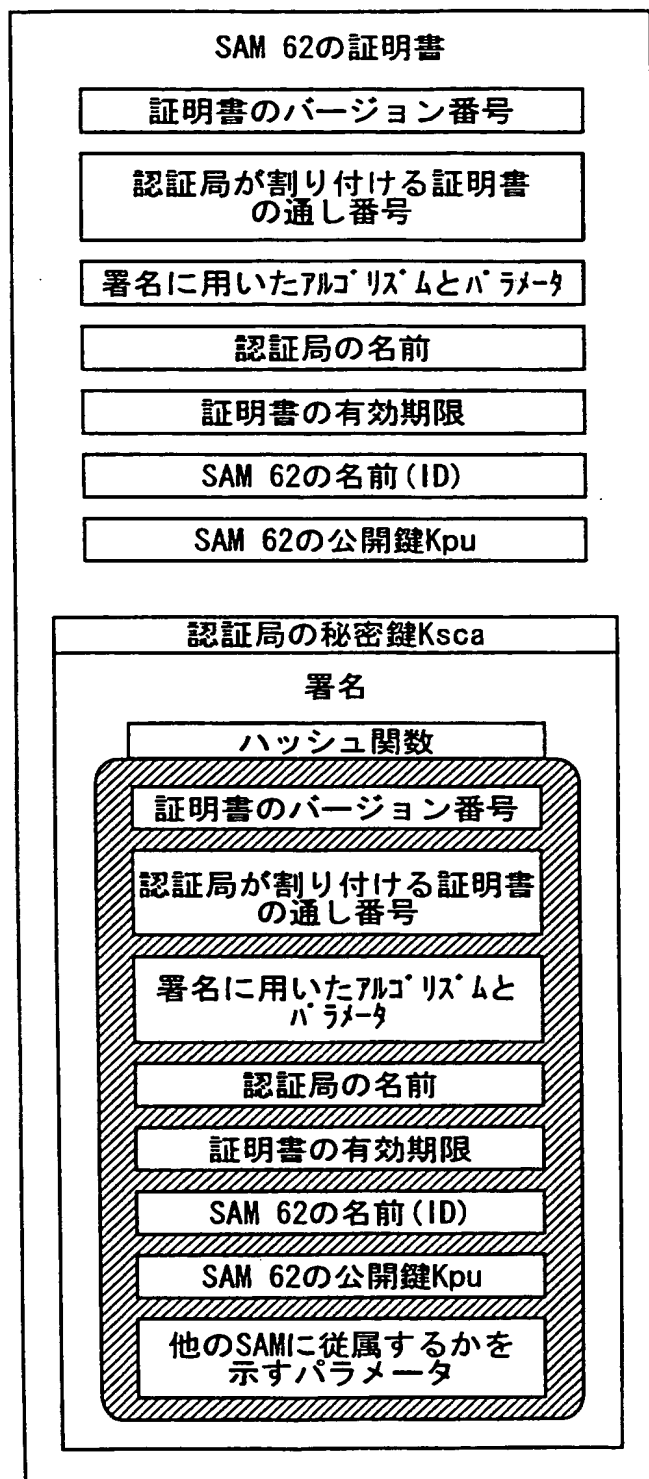


図 2 4

Best Available Copy

コンテンツのID		コンテンツAのID
コンテンツロハ'イタ'のID		コンテンツロハ'イタ'2のID
UCPのID		ucpAのID
UCPの有効期限		ucpAの有効期限
サービスロハ'イタ'のID		サービスロハ'イタ'3のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		ucsAのID
SAMのID		SAM62のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容 11のID
	形式	買い取り再生
	パラメータ	× × ×
	管理移動状態情報	管理移動元: SAM62のID、 管理移動先: SAM62のID
利用履歴		× × ×

UCSA

図 2 5

Best Available Copy

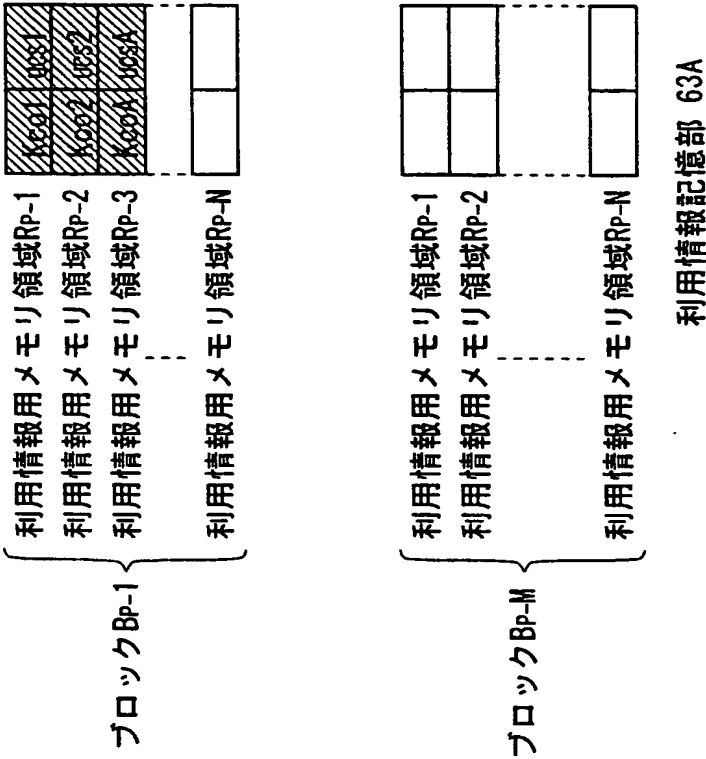


図 26

Best Available Copy

コンテンツのID		コンテンツAのID
コンテンツロバ イダ のID		コンテンツロバ イダ 2のID
UCPのID		ucPAのID
UCPの有効期限		ucPAの有効期限
サービ スロバ イダ のID		サービ スロバ イダ 3のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		ucsAのID
SAMのID		SAM62のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容11のID
	形式	買い取り再生
	パラメータ	× × ×
	管理移動状態情報	管理移動元: SAM62のID、 管理移動先: SAM62のID
課金履歴		× × ×

課金情報 A

図 2 7

Best Available Copy

SAM62の公開鍵Kpu		
SAM62の秘密鍵Ksu		
EMDサービスセンタ1の公開鍵Kpesc		
認証局の公開鍵Kpca		
保存用鍵Ksave		
3月分の配送用鍵Kd		
⋮		
SAM62証明書		
基準情報 51		
課金情報		
⋮		
検査値Hp-1	検査値Hp-2	.....
.....		検査値Hp-M

図 2 8

Best Available Copy

SAMのID		SAM62のID
機器番号		レコーダ 51の機器番号 (100番)
決済ID		ユーザの決済ID
課金の上限額		正式登録時の 課金の上限額
決済 ユーザ 情報	氏名	ユーザの氏名
	住所	ユーザの住所
	電話番号	ユーザの電話番号
	決済機関情報	ユーザの決済機関情報
	生年月日	ユーザの生年月日
	年齢	ユーザの年齢(21才)
	性別	ユーザの性別(男)
	ユーザのID	ユーザのID
	パスワード	ユーザのパスワード

利用ポイント情報	レコーダ 51の利用 ポイント情報
----------	----------------------

基準情報 51

図 2 9

Best Available Copy

レシーバ51の登録条件

レシーバ201の登録条件

SAM ID	ユーザID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態フラグ	登録条件署名	登録リスト署名
SAM62のID	ユーザのID	可	可	SAM62のID	なし	制限なし	xxxx	xxxx
SAM212のID	ユーザのID	可	不可	SAM62のID	なし	制限なし	xxxx	

リスト部

対象SAM ID

有効期限

バージョン番号

接続されている機器数

SAM62のID

xxxx

xxxx

2

対象SAM情報部

レシーバ51の登録リスト

図 30

Best Available Copy

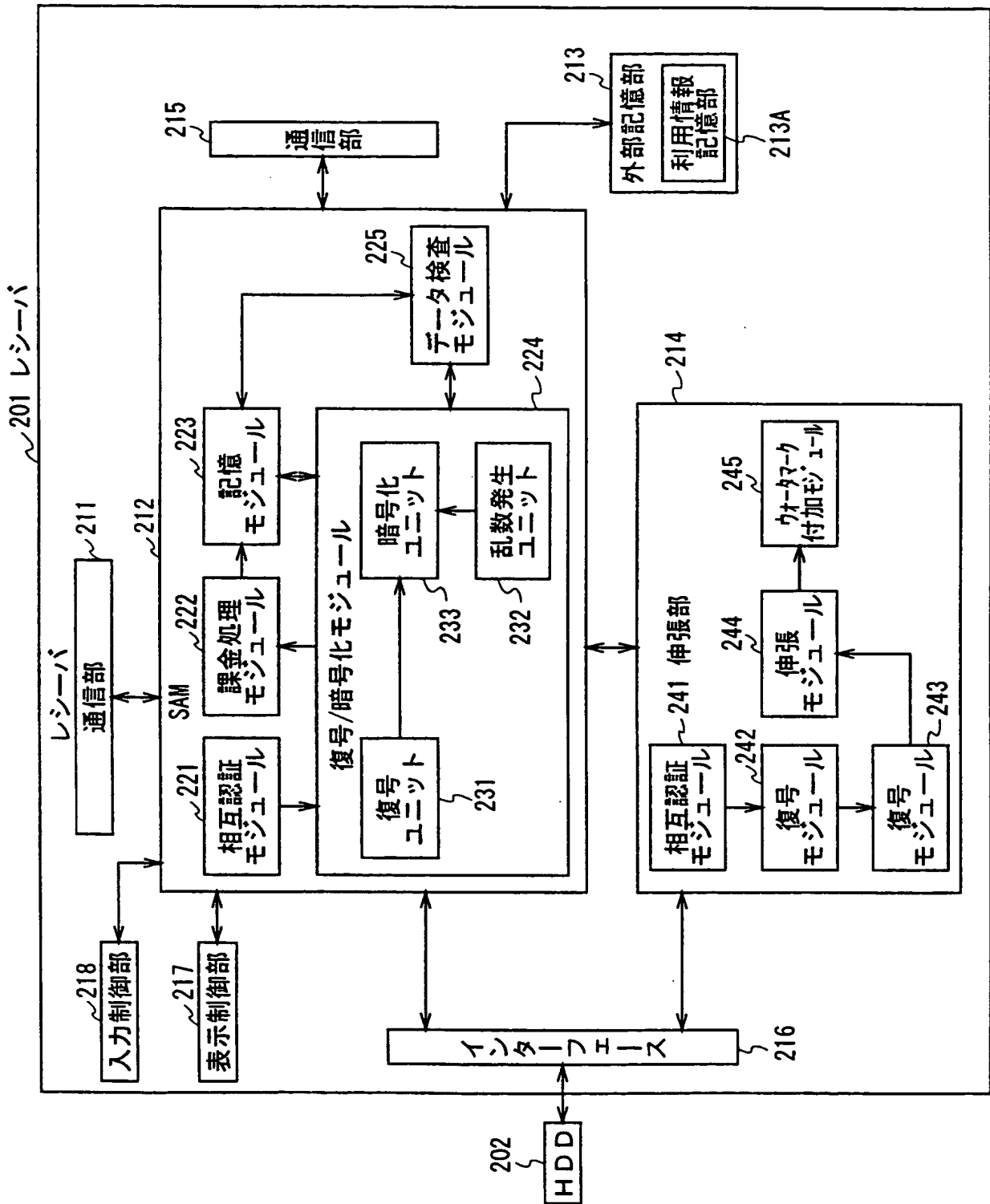


図 31

Best Available Copy

		リスト部						
SAM ID	ユーザID	購入 処理	課金 処理	課金機器	コンテンツ 供給機器	状態 フラグ	登録条件 署名	登録リスト 署名
SAM62のID	ユーザのID	可	可	SAM62のID	なし	制限 なし	××××	××××
SAM212のID	ユーザのID	可	不可	SAM62のID	なし	制限 なし	××××	

レシーバ51の登録条件

レシーバ201の登録条件

対象SAM ID

有効期限

バージョン番号

接続されている機器数

SAM212のID

××××

××××

2

対象SAM情報部

レシーバ201の登録リスト

図 3 2

Best Available Copy

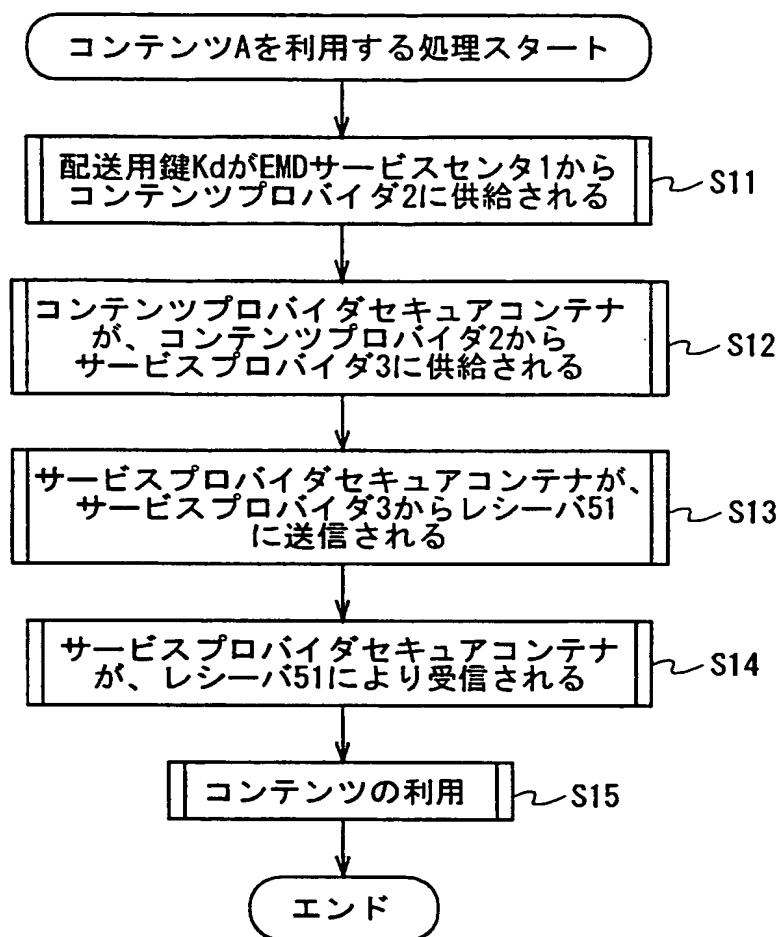


図 3 3

Best Available Copy

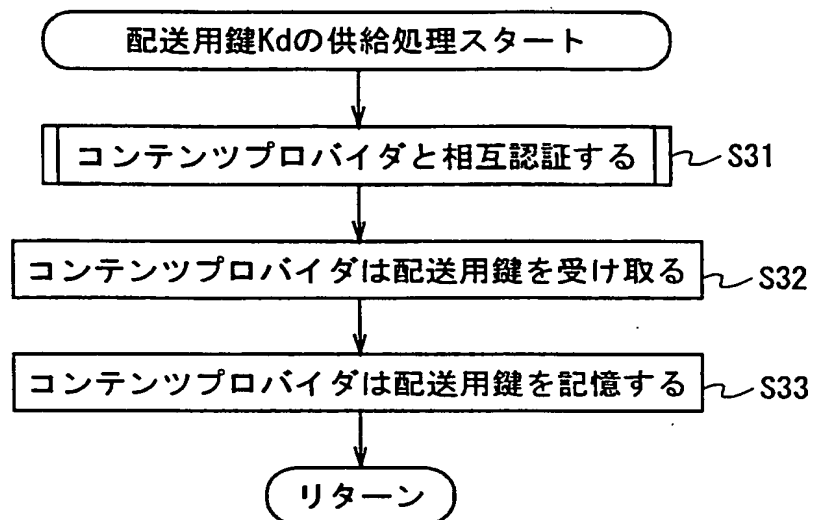


図 3 4

Best Available Copy

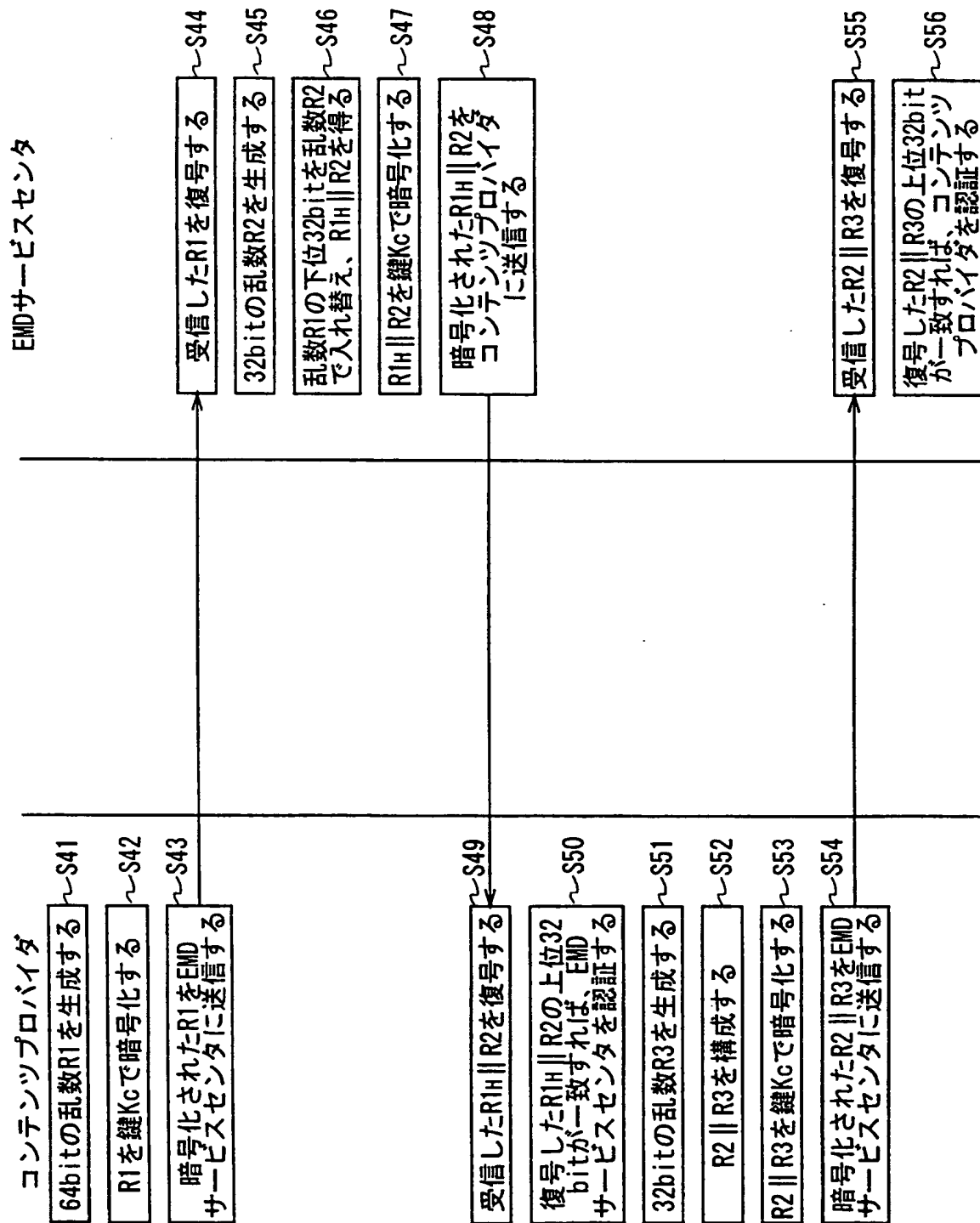


図 35

Best Available Copy

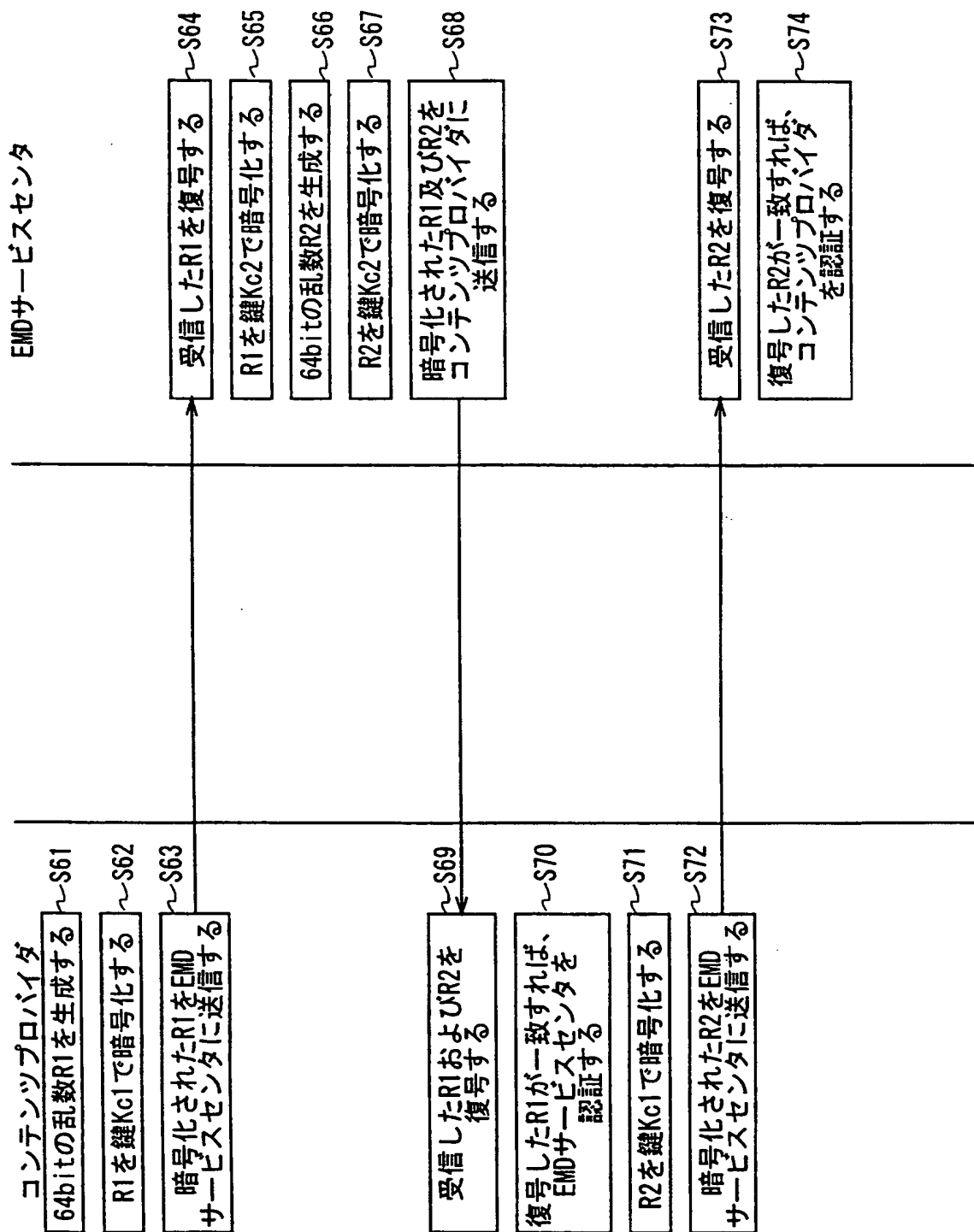


図 3 6

best Available Copy

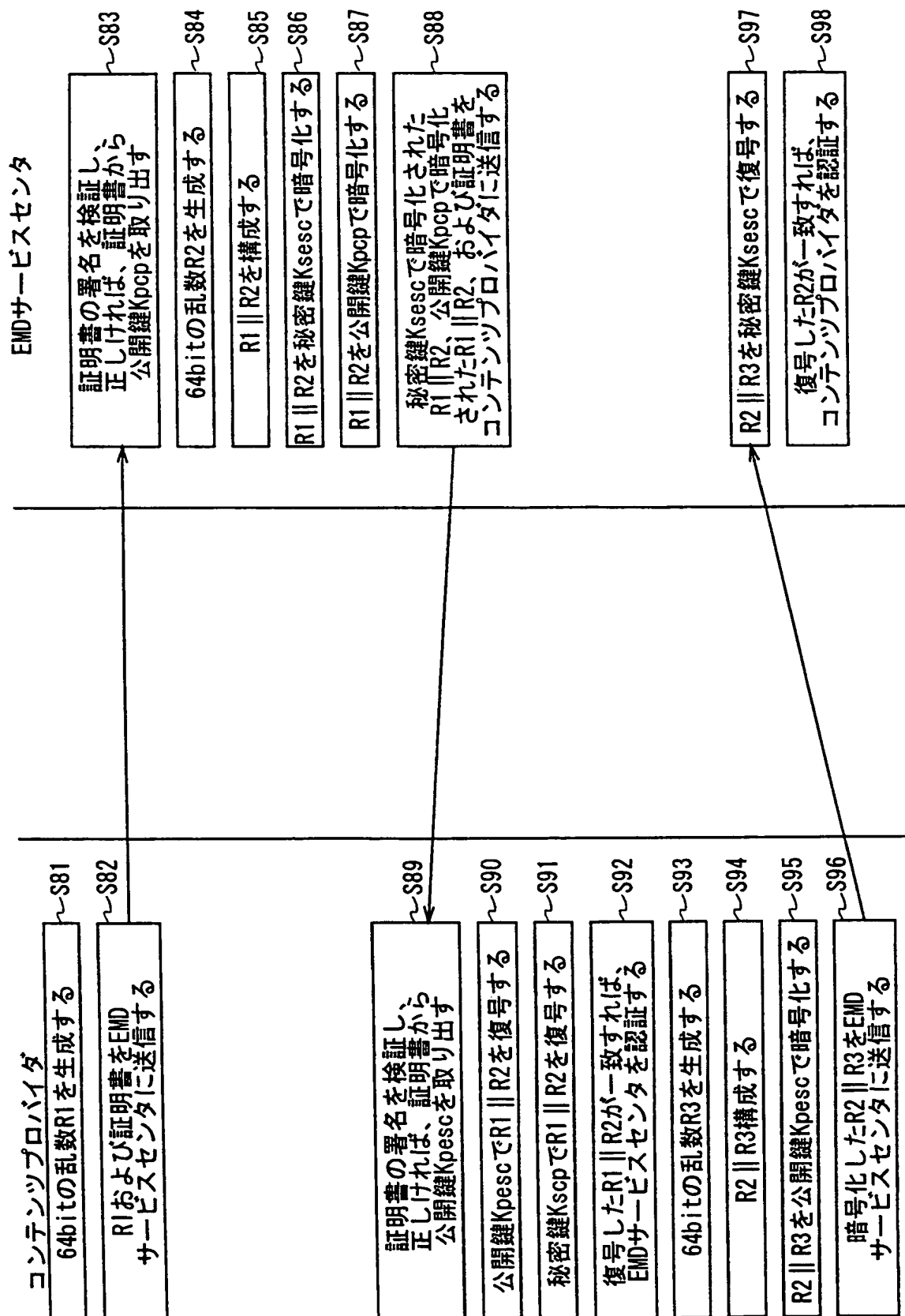


図 37

**Best Available Copy**

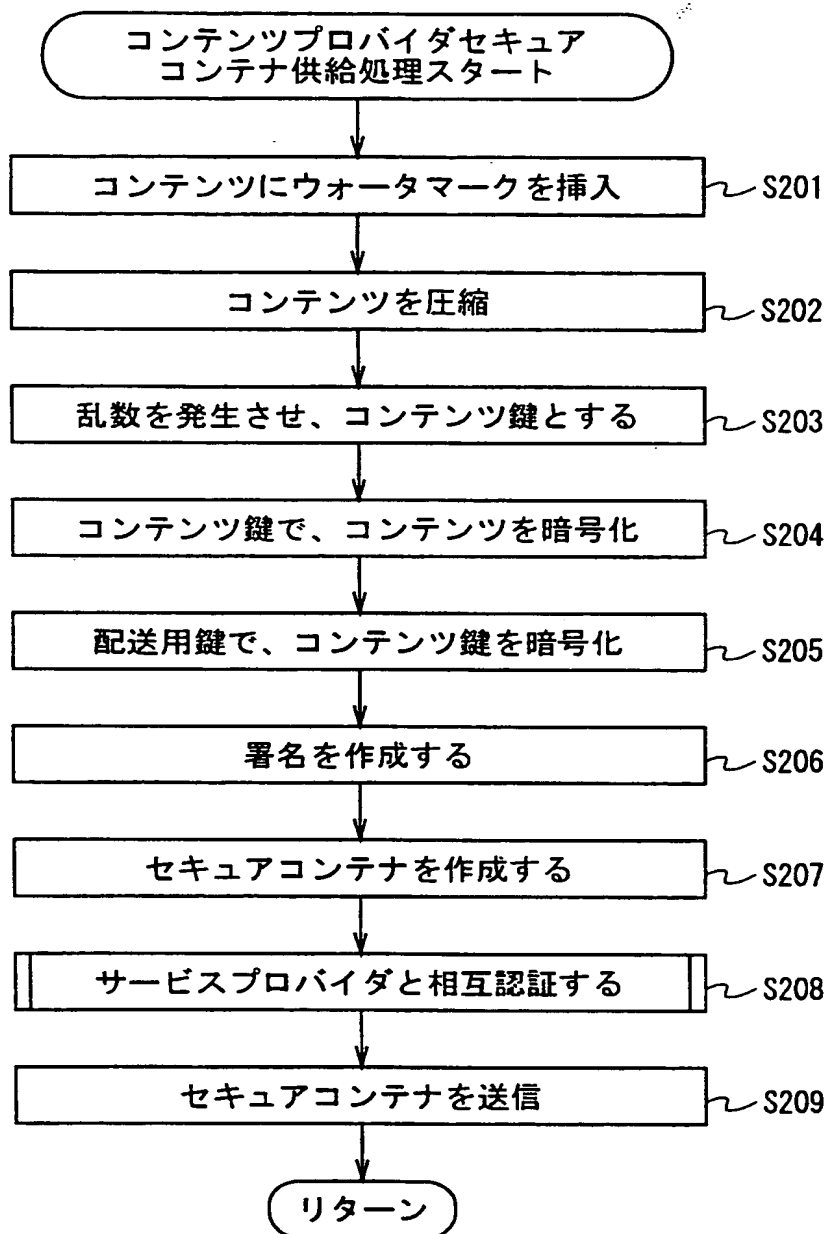


図 3 8

Best Available Copy

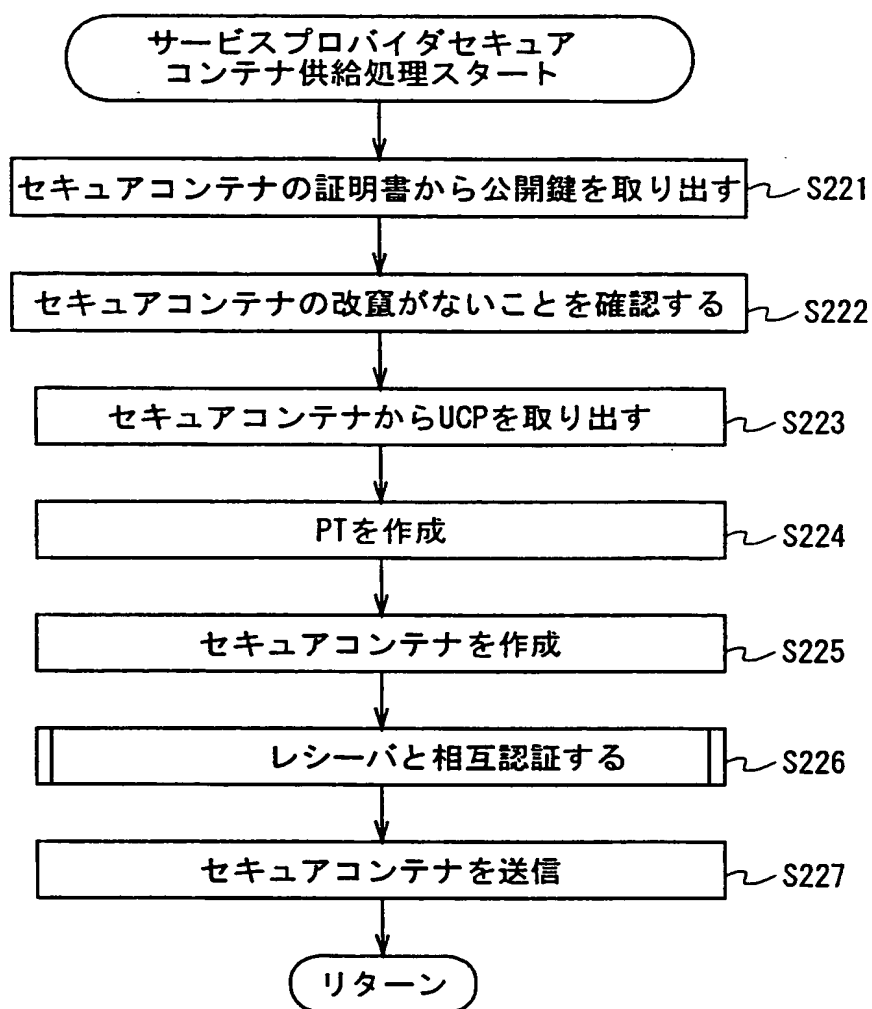


図 3 9

Best Available Copy

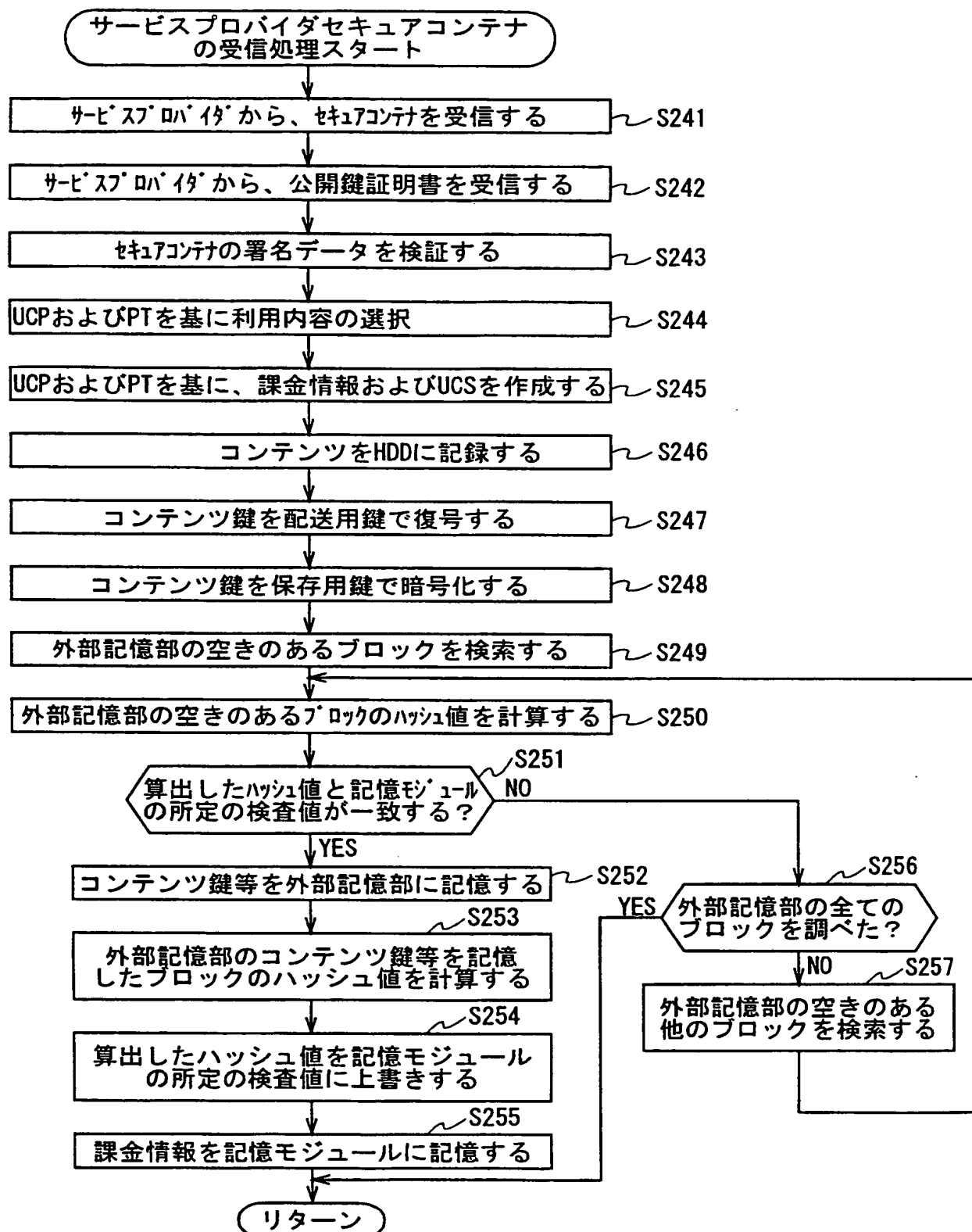


図 40

Best Available Copy

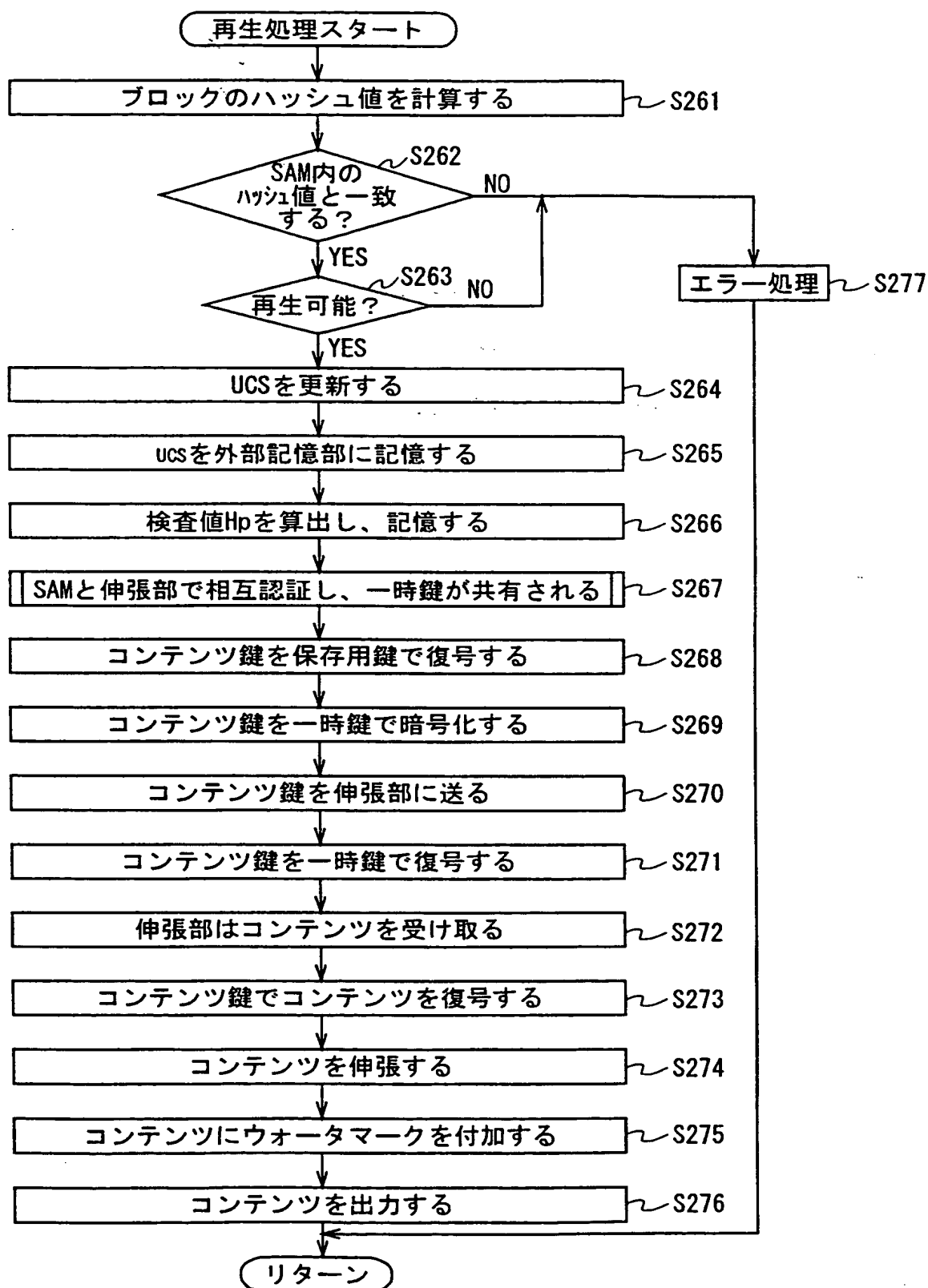


図 4 1

Best Available Copy

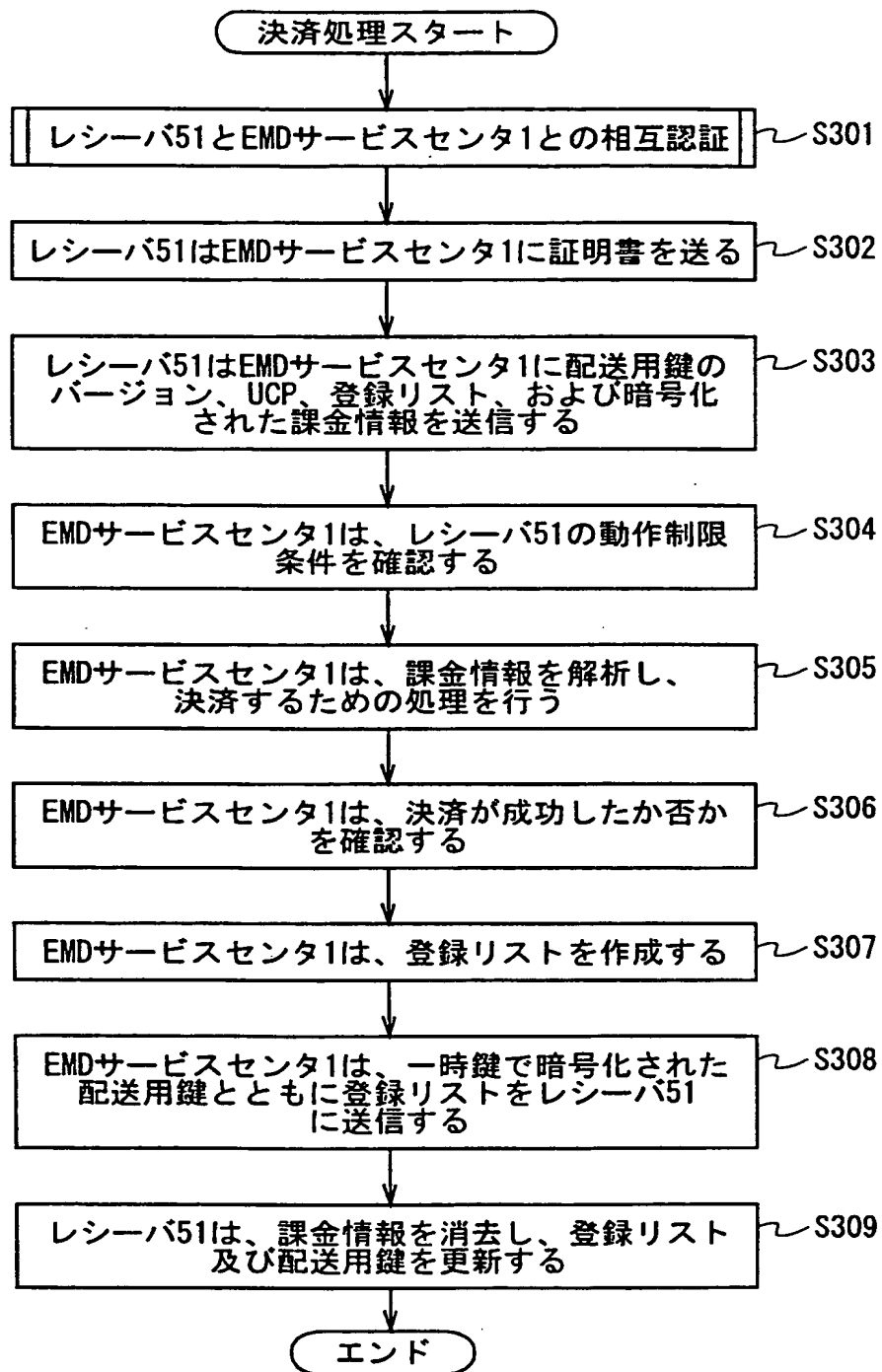


図 4 2

**Best Available Copy**

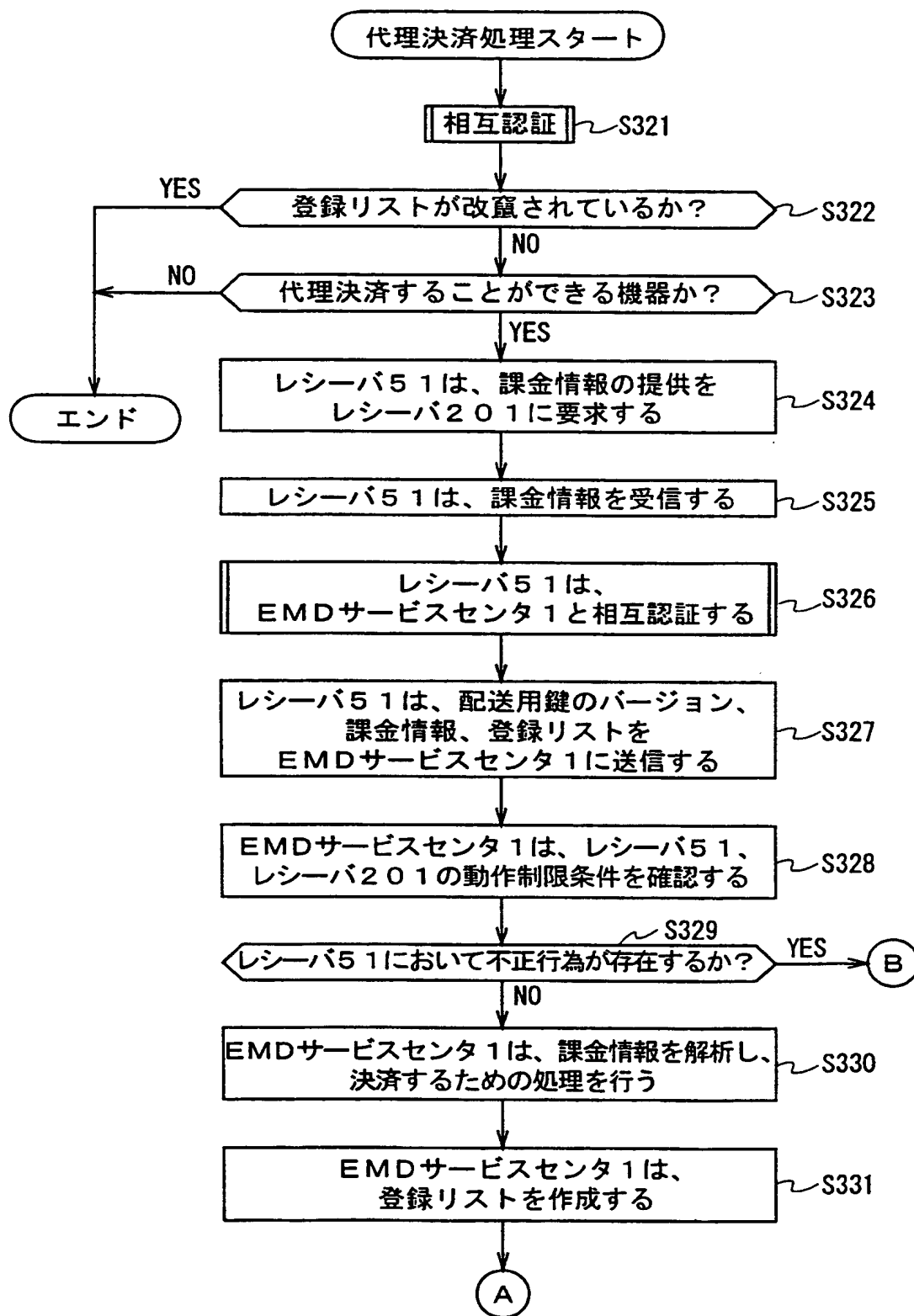


図 4 3

Best Available Copy

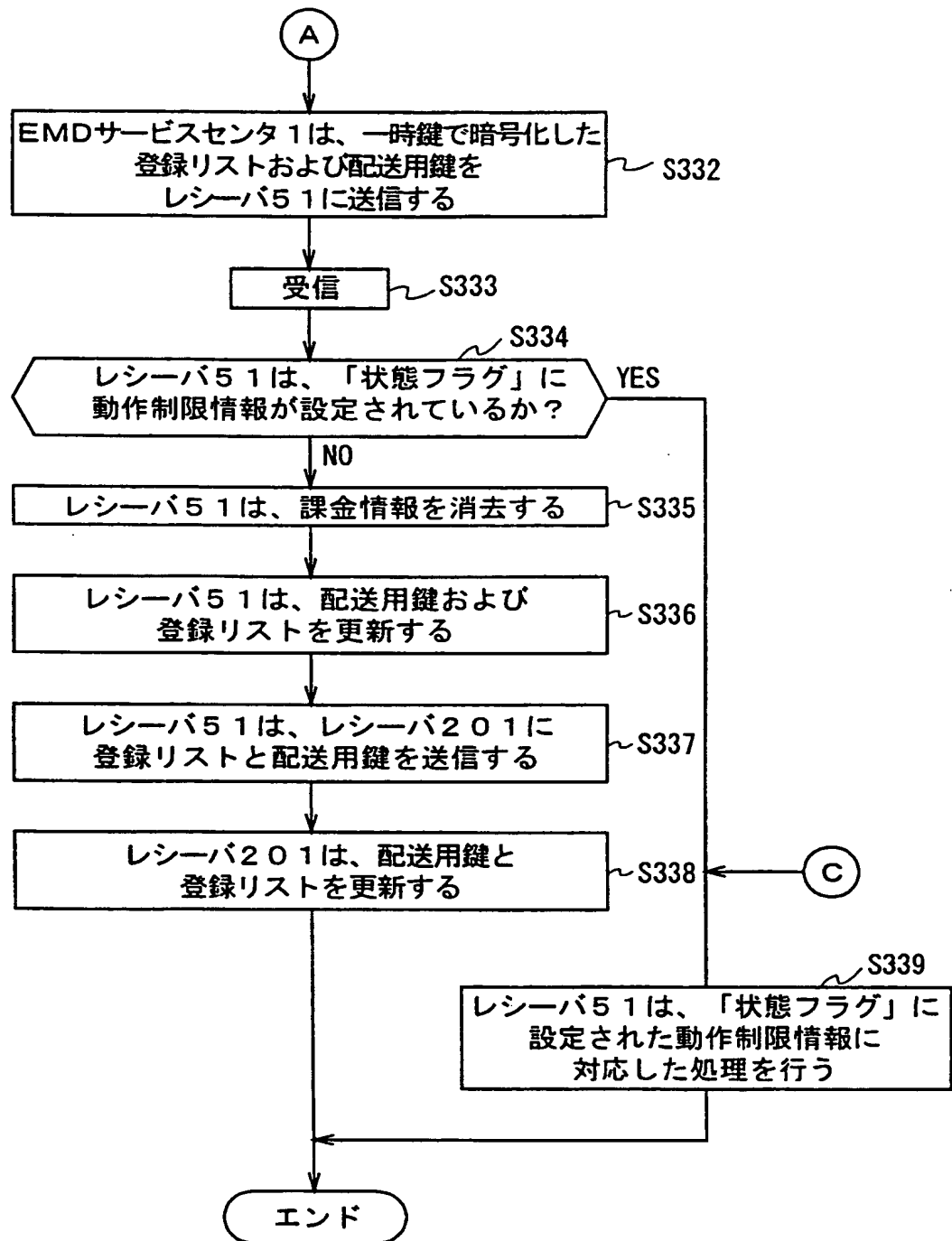


図 4 4

Best Available Copy

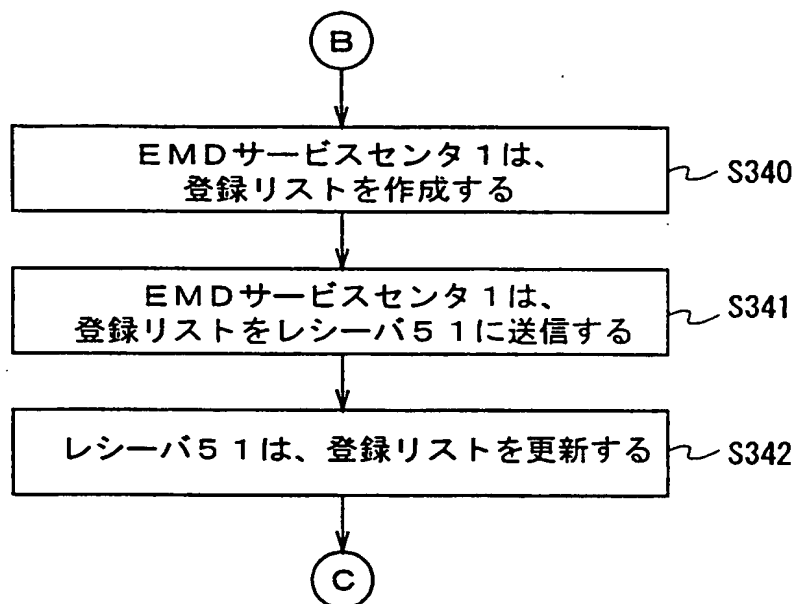
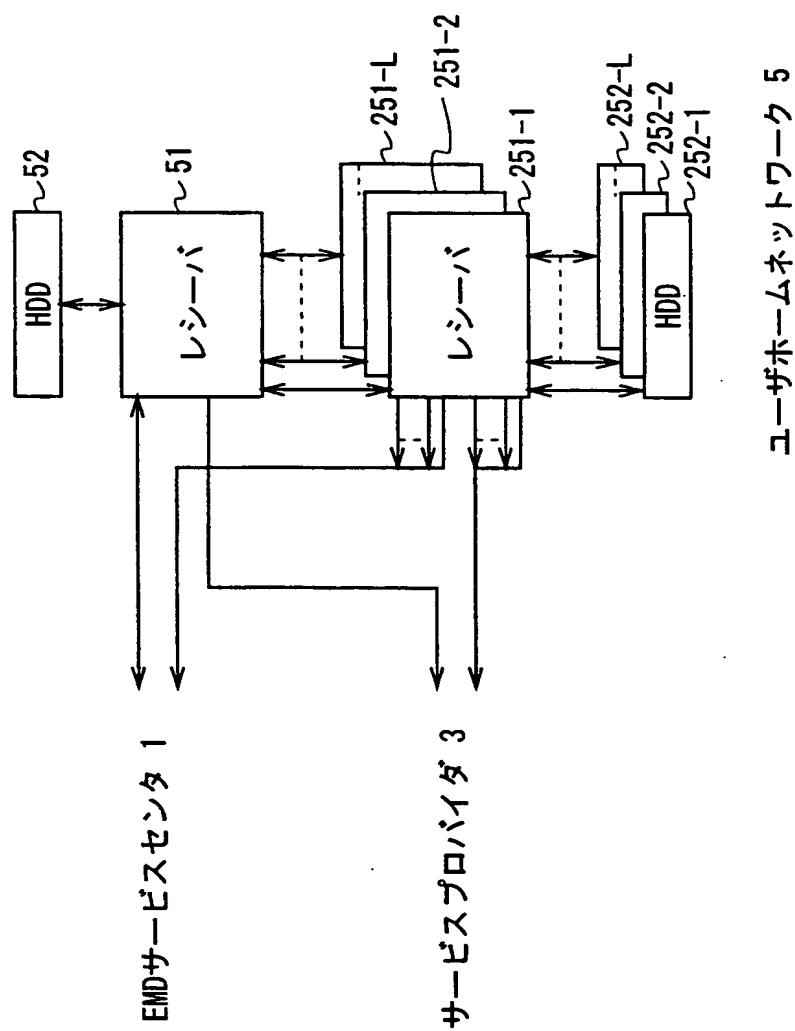


図 4 5

Best Available Copy



64

Best Available Copy

リスト部									
SAM ID	ユーザ ID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態フラグ	登録条件署名	登録リス署名	
レジャー51の登録条件	ユーザの ID	可	可	SAM62の ID	なし	制限なし	× × × ×	× × × ×	
レジャー251-1の登録条件	ユーザの ID	可	不可	SAM62の ID	なし	制限なし	× × × ×		
レジャー251-2の登録条件	ユーザの ID	可	不可	SAM62の ID	なし	制限なし	× × × ×		
...	...	...	...	...	...	...	...		

対象SAM ID

有効期限

バージョン番号

接続されている機器数

SAM62の ID

× × × ×

× × × ×

L+1

対象SAM情報部

74图

Best Available Copy

リスト部												
SAM ID	ユーザID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態フラグ	登録条件署名	登録リスト署名				
レジャー51の登録条件	ユーザのID	可	可	SAM62のID	なし	制限なし	××××	××××				
レジャー251-1の登録条件	ユーザのID	可	不可	SAM62のID	なし	制限なし	××××	××××				
レジャー251-2の登録条件	ユーザのID	可	不可	SAM62のID	なし	制限なし	××××	××××				
...	...	...	...	...	...	...	...	...				

レジャー51の登録条件

レジャー251-1の登録条件

レジャー251-2の登録条件

...

対象SAM ID

有効期限

バージョン番号

接続されている機器数

レジャー251-1のSAMのID

××××

××××

2

対象SAM情報部

図 4 8

Best Available Copy

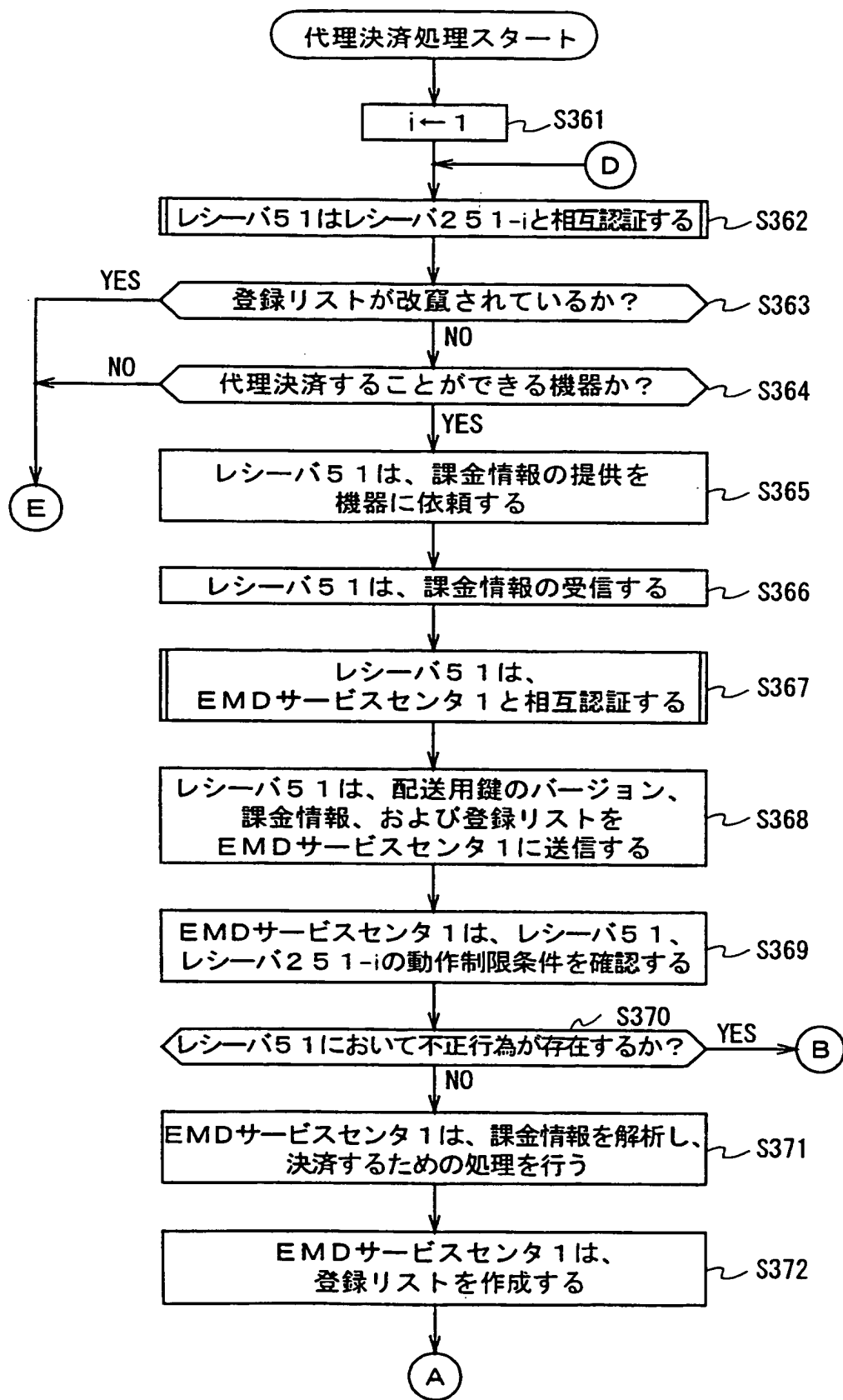


図 49

Best Available Copy

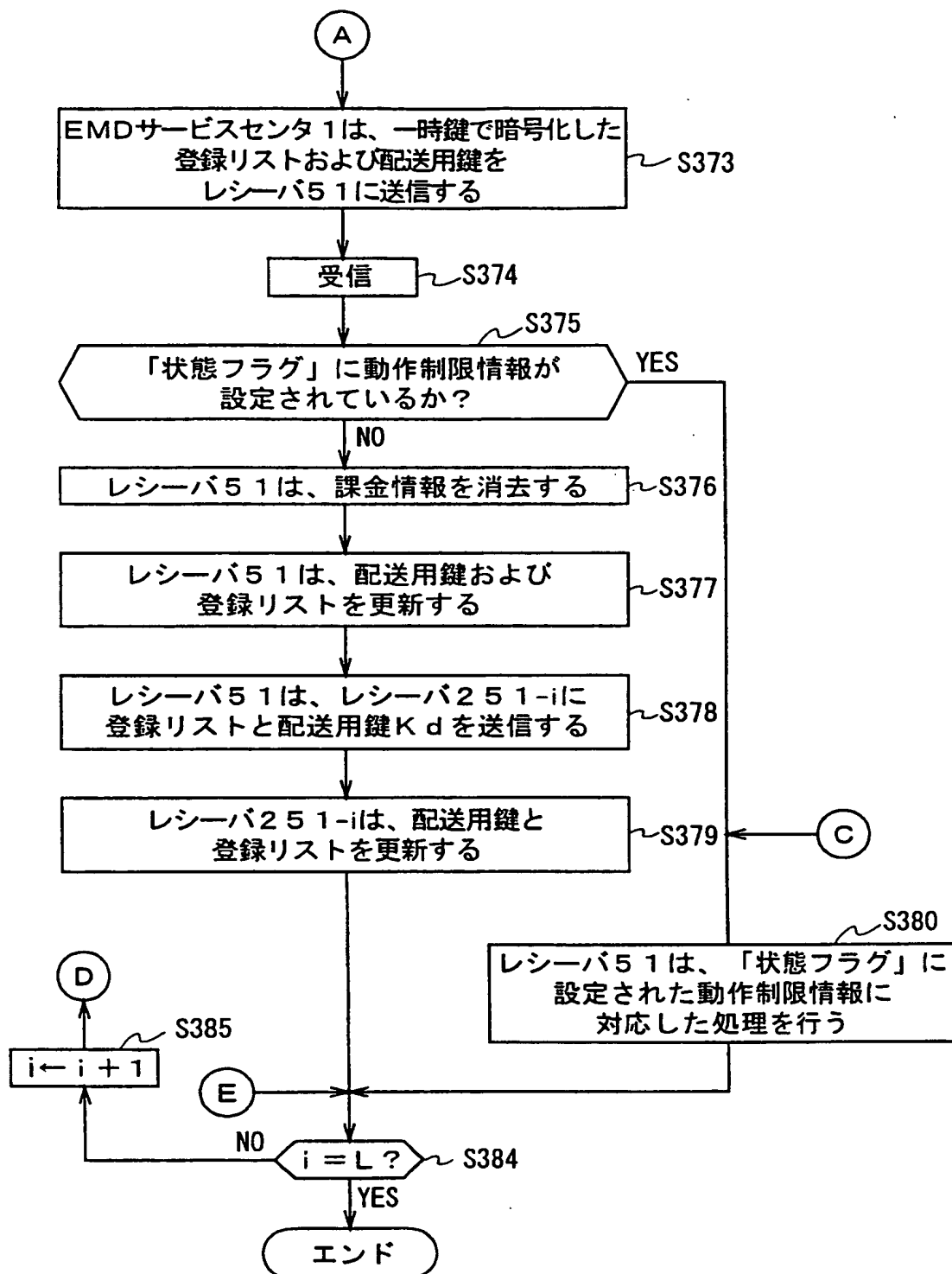


図50

Best Available Copy

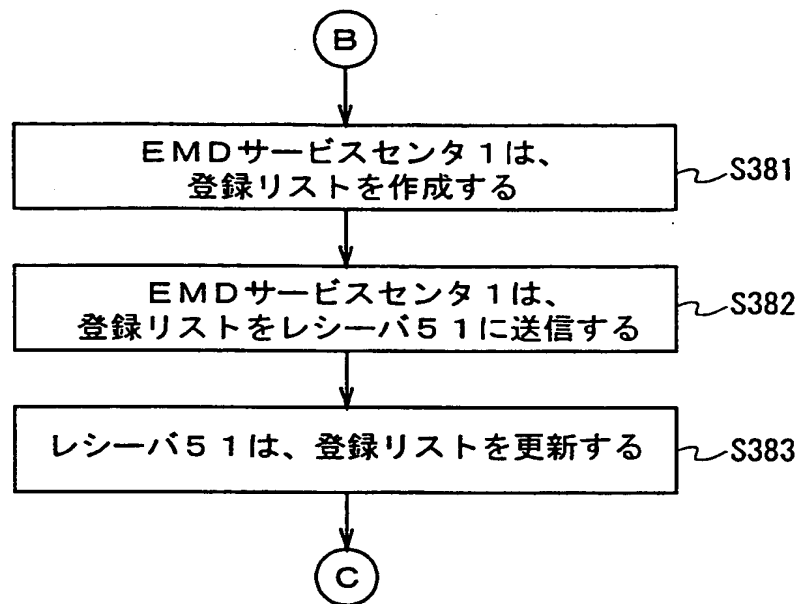
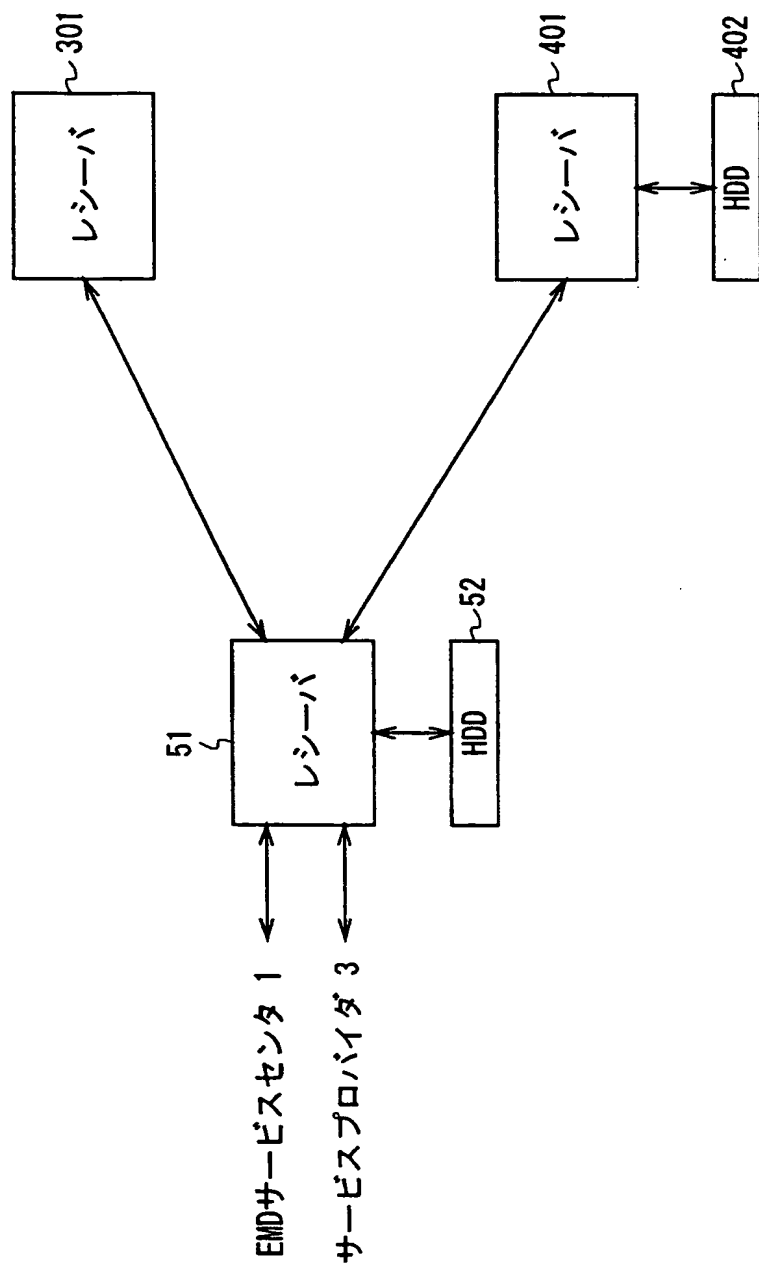


図 5 1

Best Available Copy



ユーザホームネットワーク 5

図 5 2

Best Available Copy

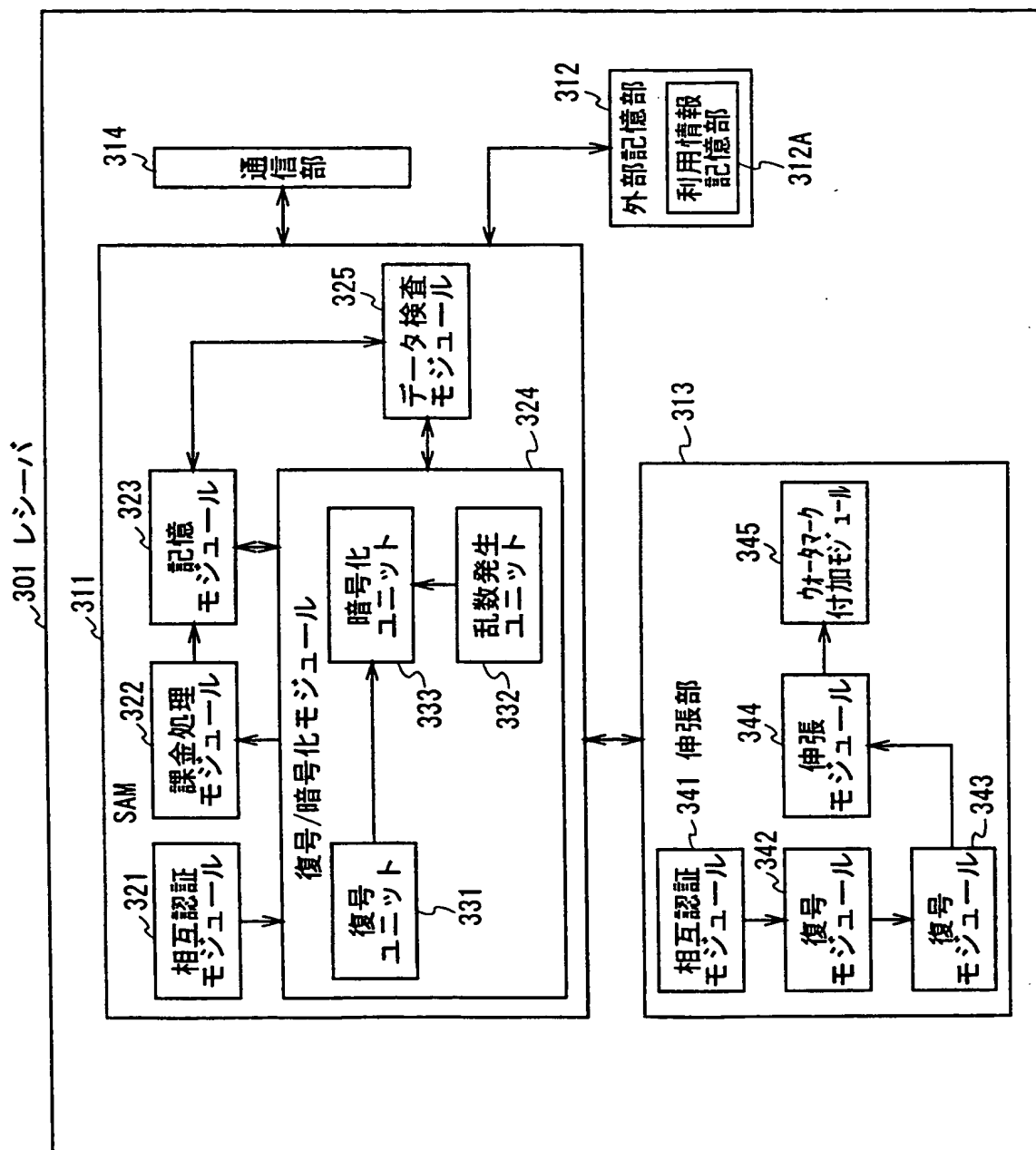


図 5 3

**Best Available Copy**

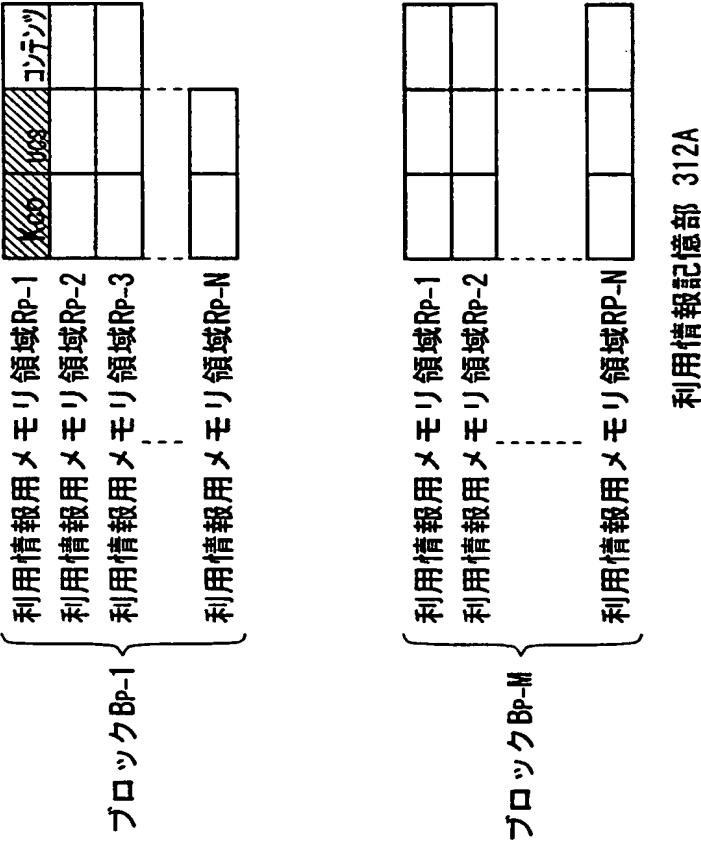


図 5 4

Best Available Copy

レシーバ301の登録条件

SAM ID	ユーザID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態フラグ	登録条件署名	登録リスト署名
SAM311のID	ユーザのID	不可	不可	なし	SAM62のID	制限なし	××××	××××

リスト部

対象SAM ID

SAM311のID

有効期限

××××

バージョン番号

××××

接続されている機器数

2

対象SAM情報部

レシーバ301に登録リスト

図 5 5

Best Available Copy

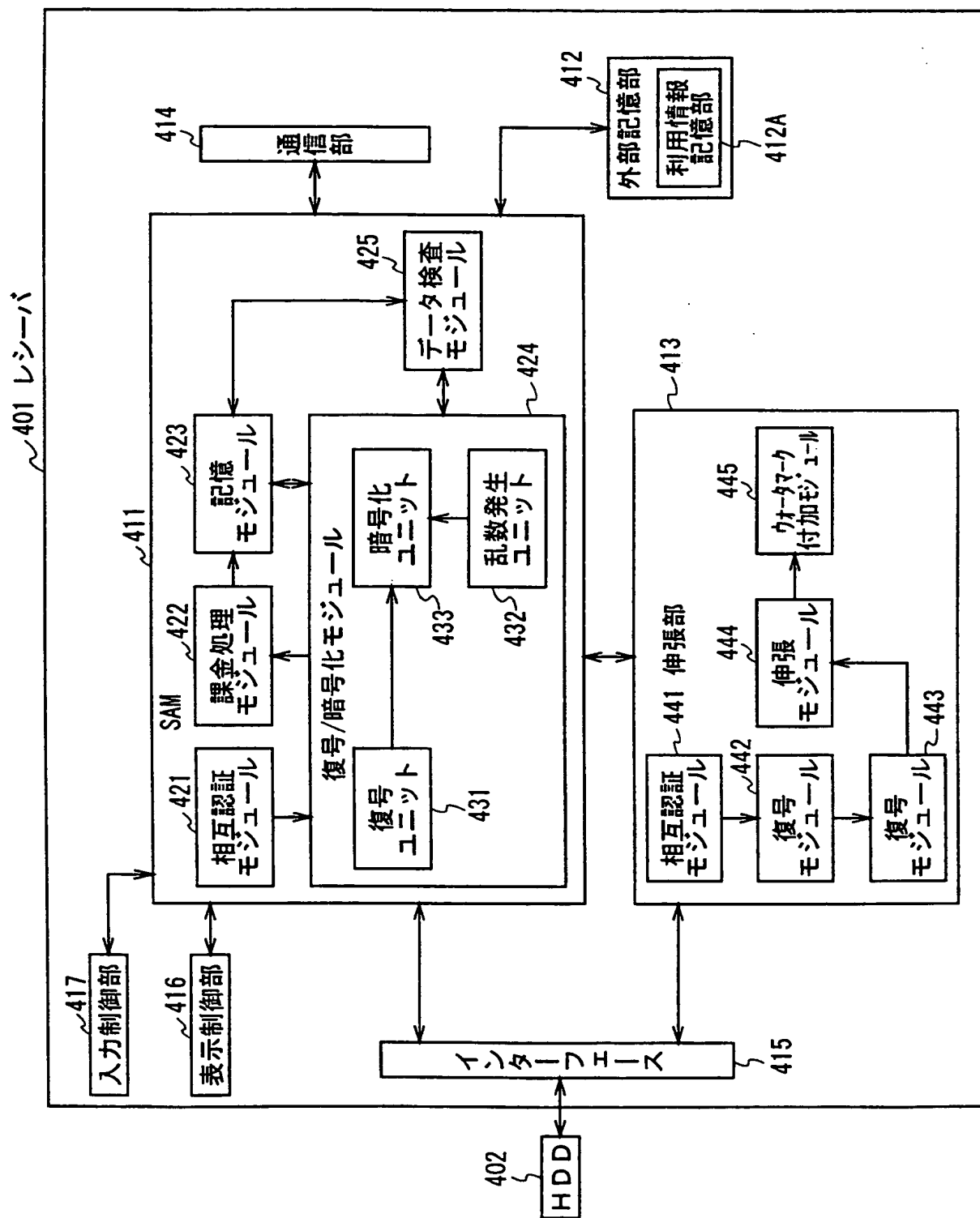


図 56

Best Available Copy

レシーバ401の登録条件

SAM ID	ユーザID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態フラグ	登録条件署名	登録リスト署名
SAM411のID	ユーザのID	不可	不可	なし	SAM62のID	制限なし	xxxxx	xxxxx

リスト部

対象SAM ID

SAM411のID

有効期限

xxxxx

バージョン番号

xxxxx

接続されている機器数

2

対象SAM情報部

レシーバ401の登録リスト

図 5 7

Best Available Copy



*Best Available Copy*

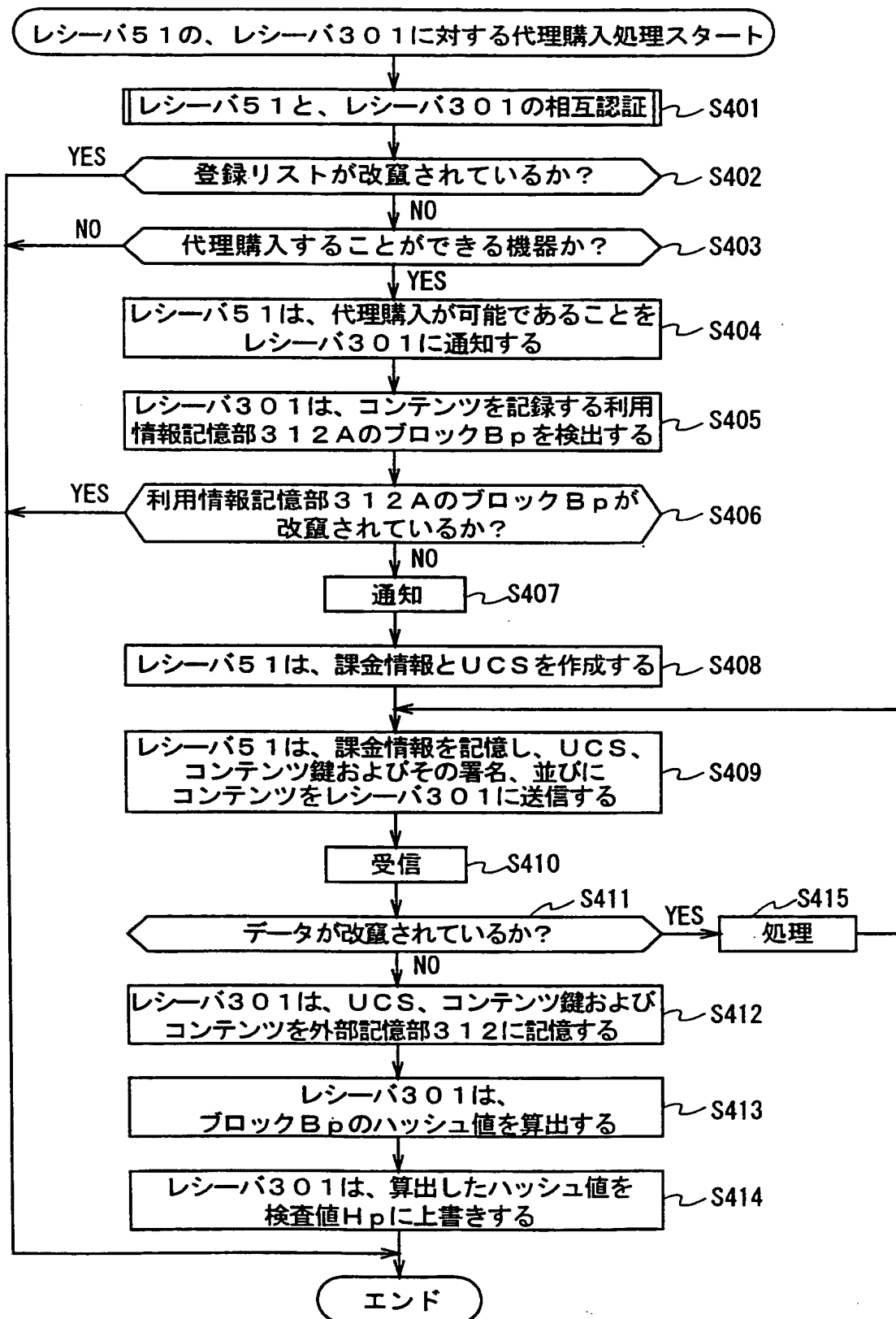
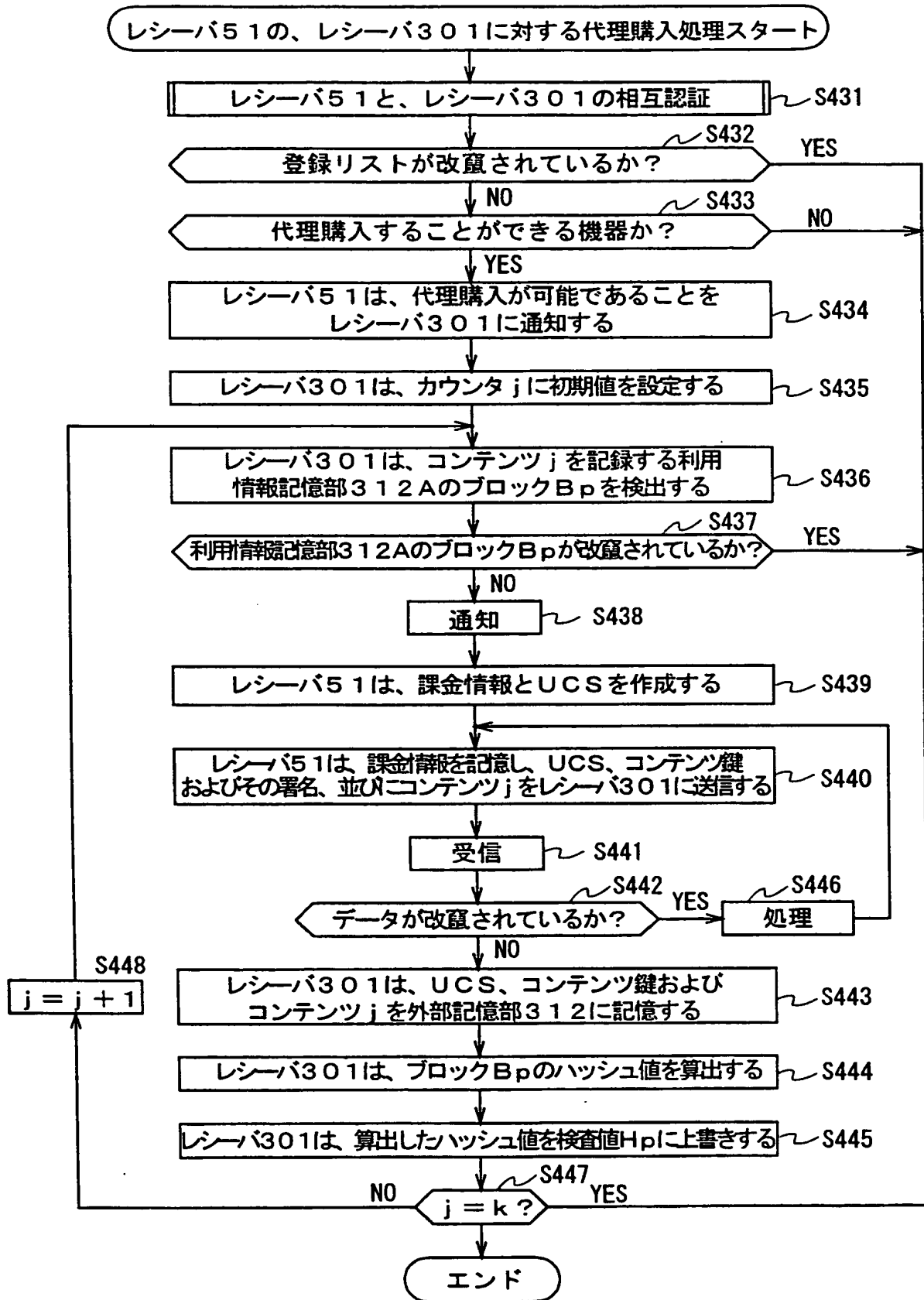
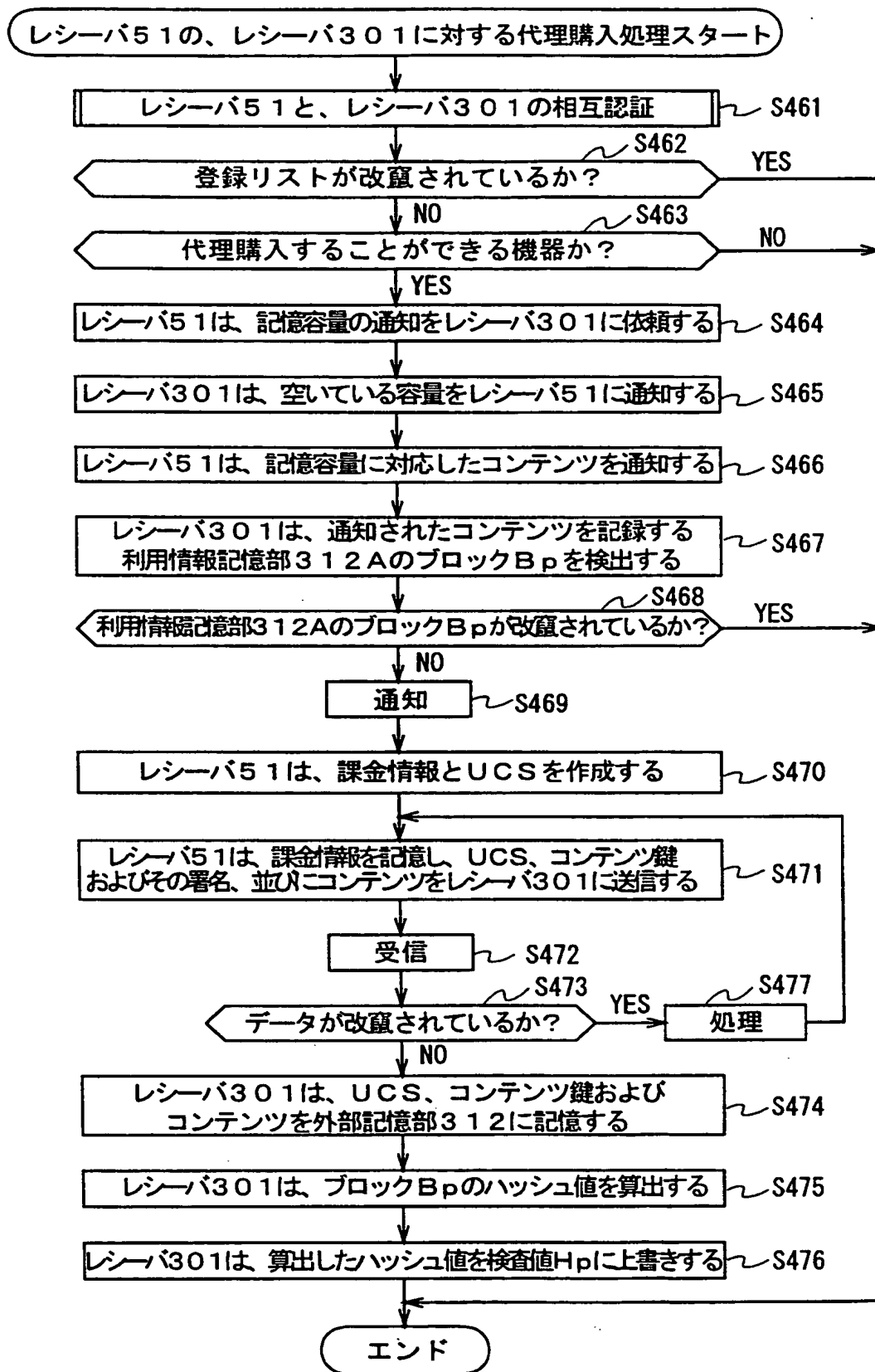


図 5 9

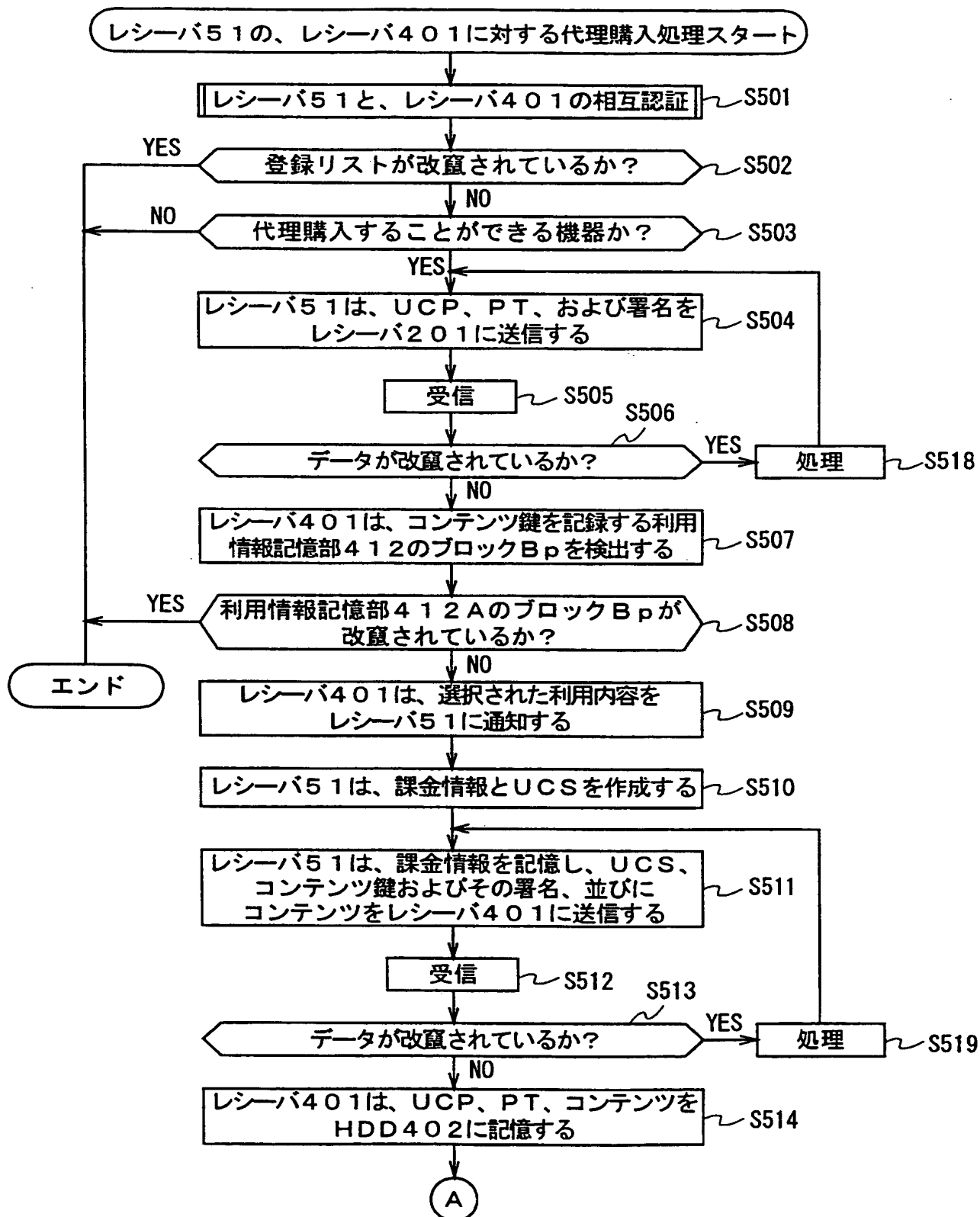
**Best Available Copy**



Best Available Copy



Best Available Copy



Best Available Copy

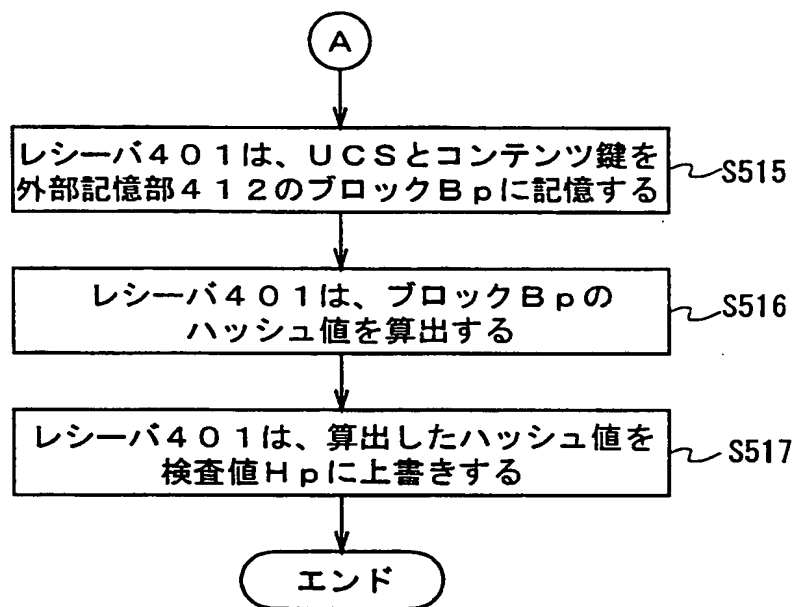


図 6 3

Best Available Copy

## 符 号 の 説 明

1……EMDサービスセンタ, 2……コンテンツプロバイダ, 3……サービスプロバイダ, 5……ユーザホームネットワーク, 11……サービスプロバイダ管理部, 12……コンテンツプロバイダ管理部, 13……著作権管理部, 14……鍵サーバ, 15……経歴データ管理部, 16……利益分配部, 17……相互認証部, 18……ユーザ管理部, 19……課金請求部, 20……出納部, 21……監査部, 31……コンテンツサーバ, 32……ウォータマーク付加部, 33……圧縮部, 34……暗号化部, 35……乱数発生部, 36……暗号化部, 37……ポリシー記憶部, 38……セキュアコンテンツ作成部, 39……相互認証部, 41……コンテンツサーバ, 42……値付け部, 43……ポリシー記憶部, 44……セキュアコンテンツ作成部, 45……相互認証部, 51……レシーバ, 52……HDD, 61……通信部, 62……SAM, 63……外部記憶部, 64……伸張部, 65……通信部, 66……インタフェース, 67……表示制御部, 68……入力制御部, 71……相互認証モジュール, 72……課金処理モジュール, 73……記憶モジュール, 74……復号/暗号化モジュール, 75……データ検査モジュール, 91……復号ユニット, 92……乱数発生ユニット, 93……暗号化ユニット, 101……相互認証モジュール, 102……復号モジュール, 103……復号モジュール, 104……伸張モジュール, 105……ウォータマーク付加モジュール, 201……レシーバ, 202……HDD, 211……通信部, 212……SAM, 213……外部記憶部, 214……伸張部, 215……通信部, 216……インタフェース, 217……表示制御部, 218……入力制御部, 221……相互認証モジュール, 222……課金処理モジュール, 223……記憶モジュール, 224……

Best Available Copy

…復号／暗号化モジュール， 2 2 5 ……データ検査モジュール， 2 3 1 ……  
復号ユニット， 2 3 2 ……乱数発生ユニット， 2 3 3 ……暗号化ユニット，  
2 4 1 ……相互認証モジュール， 2 4 2 ……復号モジュール， 2 4 3 ……復  
号モジュール， 2 4 4 ……伸張モジュール， 2 4 5 ……ウォータマーク付加  
モジュール， 3 0 1 ……レシーバ， 3 1 1 ……S A M， 3 1 2 ……外部記  
憶部， 3 1 3 ……伸張部， 3 1 4 ……通信部， 3 2 1 ……相互認証モジュ  
ール， 3 2 2 ……課金処理モジュール， 3 2 3 ……記憶モジュール， 3 2  
4 ……復号／暗号化モジュール， 3 2 5 ……データ検査モジュール， 3 3 1  
……復号ユニット， 3 3 2 ……乱数発生ユニット， 3 3 3 ……暗号化ユニッ  
ト， 3 4 1 ……相互認証モジュール， 3 4 2 ……復号モジュール， 3 4 3  
……復号モジュール， 3 4 4 ……伸張モジュール， 3 4 5 ……ウォータマー  
ク付加モジュール， 4 0 1 ……レシーバ， 4 0 2 ……H D D， 4 1 1 ……  
S A M， 4 1 2 ……外部記憶部， 4 1 3 ……伸張部， 4 1 4 ……通信部，  
4 1 5 ……インタフェース， 4 1 6 ……表示制御部， 4 1 7 ……入力制御部  
， 4 2 1 ……相互認証モジュール， 4 2 2 ……課金処理モジュール， 4 2  
3 ……記憶モジュール， 4 2 4 ……復号／暗号化モジュール， 4 2 5 ……デ  
ータ検査モジュール， 4 3 1 ……復号ユニット， 4 3 2 ……乱数発生ユニッ  
ト， 4 3 3 ……暗号化ユニット， 4 4 1 ……相互認証モジュール， 4 4 2  
……復号モジュール， 4 4 3 ……復号モジュール， 4 4 4 ……伸張モジュ  
ール， 4 4 5 ……ウォータマーク付加モジュール

Best Available Copy

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/02291

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G06F17/60, G06F13/00, G09C1/00, H04L9/08, G06F15/00, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2000  
Kokai Jitsuyo Shinan Koho 1971-2000 Toroku Jitsuyo Shinan Koho 1994-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO, 96/27155, A2 (InerTrust Technologies Corp.) 6 September, 1996 (06.09.96) &JP, 10-512074, A	1-7
A	Jinbun Kagaku to Computer, Vols. 36 to 38, November, 1997, Seiji Kawahara, "Chosaku Ken Shori Gijutsu no Saikin no Doko", pp.43-48	1-7

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance  
"E" earlier document but published on or after the international filing date  
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)  
"O" document referring to an oral disclosure, use, exhibition or other means  
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art  
"&" document member of the same patent family

Date of the actual completion of the international search  
24 May, 2000 (24.05.00)

Date of mailing of the international search report  
13 June, 2000 (13.06.00)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

Best Available Copy

## 国際調査報告

国際出願番号 PCT/JPO0/02291

A. 発明の属する分野の分類 (国際特許分類 (IPC))		
Int. Cl <sup>7</sup> G06F17/60		
B. 調査を行った分野		
調査を行った最小限資料 (国際特許分類 (IPC))		
Int. Cl <sup>7</sup> G06F17/60 G06F13/00 G09C1/00 H04L9/08 G06F15/00 H04L9/32		
最小限資料以外の資料で調査を行った分野に含まれるもの		
日本国実用新案公報 1926-1996年 日本国公開実用新案公報 1971-2000年 日本国実用新案登録公報 1996-2000年 日本国登録実用新案公報 1994-2000年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)		
JICSTファイル(JOIS)		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	WO, 96/27155, A2(InerTrust Technologies Corp.) 6. 9月. 1996 (06. 0 9. 96)&JP, 10-512074, A	1-7
A	人文科学とコンピュータ, 第36-8巻, 11月. 1997 河原正治「著作権 処理技術の最近の動向」p. 43-48	1-7
<input type="checkbox"/> C欄の続きにも文献が列举されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日	24. 05. 00	国際調査報告の発送日 13. 06. 00
国際調査機関の名称及びあて先 日本国特許庁 (ISA/J P) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 岩間 直純	5L 9287
電話番号 03-3581-1101		内線 3562

Best Available Copy